INFORMATION & SECURITY

An International Journal

Volume 19, 2006

IT, Emerging Commercial Capabilities, Terrorism

Edited by
Goran Johnson

ProCon Ltd., Sofia 2006

Content *I&S*

ADVANCED INFORMATION TECHNOLOGY AND TERRORISM

Advances in commercial information technology and the rising threat of global terrorism are two of the most important influences on nations and their economies. Computing and communications services offered commercially nowadays provide capabilities with global reach that formerly were available only to the most advanced military organizations. Mobile user services, including 3G mobile telephones and broadband wireless networks, provide for wide range of applications previously constrained to static networks and desktop computers. Any group of users with sufficient funding can purchase off-the-shelf capabilities for network enabled operations, including video teleconferencing, shared white boarding, image capture and dissemination, and robust information protection.

The result is an "information battlespace" as an essential playing field for nations and their terrorist opponents. Since governments, their military and commercial sectors are major players in the war on terrorism, it is essential that they understand how to make best use of the new and emerging technologies while denying critical capabilities to terrorist organizations. Cooperation among the military and commercial sectors and across the nations will be necessary to reach this understanding so that appropriate actions can be taken in the commercial marketplace to steer technology in ways that are most productive and supportive of peace, stability, and prosperity.

To reflect the respective conceptual, doctrinal, technological, and organizational developments and to facilitate adequate responses by governments and industry, the Editorial Board of *Information & Security: An International Journal* (I&S), jointly with CITMO.net, decided to prepare a special I&S issue on IT, emerging commercial capabilities, and terrorism. As a result, this volume reflects ideas, concepts and approaches discussed during the international conference on "*Commercial Information Technologies for Military Operations*" (CITMO-2005) that took place in Plovdiv, Bulgaria, in the period 15-17 June 2005. The conference explored approaches and presented recommendations for:

- Implementation of available and appropriate technologies;

- R&D that could support development of IT and which could overcome obvious gaps;
- A strategy to coevolve the policy and IT in near-term toward achieving common goals.

This volume has two main parts. The first part starts with a look at how terrorists use Internet and what are the opportunities to counter this use without jeopardizing democratic principles and economic development. It then presents lessons learned in the use of commercial technologies in preparing our societies to respond to terrorist acts and other disasters. The final article in the first part explores emerging technologies for iris-based recognition and possible applications to enhance the security of variety of public and private facilities.

The second part covers comprehensively the roles of the military in countering terrorism. Three articles look respectively at the response of NATO to the events of September 11, 2001, missions and tasks of special operations forces in countering terrorist activity on own territory, and the responses to maritime terrorism (which, as the authors argue, shares many features with piracy at sea). All three articles commend on needs and requirements of military and other governmental organizations that could be met with commercial-off-the-shelf technologies.

This special issue provides also a comprehensive, up-to-date list with on-line resources on counterterrorism, important policy documents, related journals, institutions, technologies and scientific support, resource repositories, as well as some milestone publications.

The reader will not find answers to all related questions in this issue. We believe, though, that this I&S volume will provide ideas and novel concepts, analysis of approaches and experience.

Information & Security

Advanced Commercial IT and Terrorism

- Terrorist ‘Use’ of the Internet and Fighting Back
- Building a Sound and Flexible Emergency Response System: Hard Won Lessons in Disaster Management
- Research and Development of an Iris-Based Recognition System for Identification and Secure Authentication

TERRORIST 'USE' OF THE INTERNET AND FIGHTING BACK

Maura CONWAY

Abstract: The Internet is a powerful political instrument, which is increasingly employed by terrorists to forward their goals. The five most prominent contemporary terrorist uses of the Net are information provision, financing, networking, recruitment, and information gathering. This article describes and explains each of these uses and is illustrated with examples of each. The final section of the paper describes the responses of government, law enforcement, intelligence agencies, and others to the terrorism-Internet nexus.

Keywords: Terrorism, Internet, Terrorist Financing, Terrorist Networking, Terrorist Recruitment, Counter-Terrorism.

"Terrorists use the Internet just like everybody else"
Richard Clarke (2004) [1]

Introduction

With over 600 million Internet users worldwide in 2005, today the Internet is recognized as a powerful political instrument. David Resnick has identified three types of Internet politics [2]:

- *Politics Within the Net*: This refers to the political life of cyber-communities and other Internet activities that have minimal impact on life off the Net.
- *Politics Which Impacts the Net*: This refers to the host of public policy issues raised by the Internet both as a new form of mass communication and a vehicle for commerce.
- *Political Uses of the Net*: This refers to the employment of the Internet by ordinary citizens, political activists, organised interests, governments, and others to achieve political goals having little or nothing to do with the Internet *per se* (i.e. to influence political activities offline).

INFORMATION & SECURITY. An International Journal, Vol.19, 2006, 9-30.

This paper is centrally concerned with 'Political Uses of the Net,' specifically the use(s) made of the Internet by terrorist groups, a subject that to date has been the focus of only a very small amount of substantive social science research.

What are terrorist groups attempting to do by gaining a foothold in cyberspace? In 1997, Wayne Rash, in his *Politics on the Nets*, posited eight uses of the Net that he foresaw political groups adopting. He described these as tactical communications, organization, recruitment, fundraising, strategic positioning, media relations, affinity connections, and international connections.[3] Although Rash did not identify terrorists as a specific political Internet user group, his list of uses is broadly similar to those later developed by authors concerned with the narrower issue of terrorist use of the Net (see Table 1). In 1999, for example, Steve Furnell and Matthew Warren described the core terrorist uses of the Net as propaganda/ publicity, fundraising, information dissemination, and secure communications.[4] Fred Cohen presents his readers with a broadly similar list of uses.[5] Timothy Thomas, on the other hand, presents a more detailed rendition of terrorist uses of the Net. In his article 'Al Qaeda and the Internet: The Danger of "Cyberplanning,"' which appeared in the US Army journal *Parameters* in 2003, Thomas discusses some sixteen potential uses of the Internet by terrorists.[6] Thomas does not adopt the use paradigm but refers instead to what he dubs "cyberplanning"—"the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed" [7]—which nonetheless shares sufficient similarities with the use approach as to be almost indistinguishable from it. Finally, in a recent report for the United States Institute of Peace entitled *WWW.terror.net: How Modern Terrorism Uses the Internet*, Gabriel Weimann identifies eight different ways in which, he says, terrorists currently use the Internet. These are psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, information sharing, and planning and coordination.[8]

There is considerable overlap amongst the terrorist uses of the Net identified by the different authors in Table 1.[9] While twenty-two different categories of use are mentioned, often authors are simply using different terms to refer to the same issues. This is clearest in terms of the identity shared by the concepts 'fundraising' and 'finance,' but also relates to the concepts 'information gathering' and 'data mining,' for example. Given such overlaps, the analysis below relies on what have been determined to be the five core terrorist uses of the Internet: information provision, financing, networking, recruitment, and information gathering. Each of the uses identified in Table 1 fits into one of these categories or its sub-categories. All four authors mentioned identify resource generation along with information provision, particularly propaganda, as primary terrorist uses of the Internet. I have subsumed a number of other issues, including secure communication and planning, under the heading 'Networking.'

Table 1: Core Terrorist Uses of the Internet.

Author(s)	*Furnell & Warren* [10]	*Cohen* [11]	*Thomas* [12]	*Weimann* [13]
Uses	Propaganda & Publicity Fundraising Information Dissemination Secure Communications	Planning Finance Coordination & Operations Political Action Propaganda	Profiling Propaganda Anonymous/ Covert Communication Generating "Cyberfear" Finance Command & Control Mobilisation & Recruitment Information Gathering Mitigation of Risk Theft/ Manipulation of Data Offensive Use Misinformation	Psychological Warfare Publicity & Propaganda Data Mining Fundraising Recruitment & Mobilisation Networking Sharing Information Planning & Coordination

Finally, although recruitment is mentioned by just two of the authors discussed here,[14] there is evidence to support the view that the Internet has been utilized to promote participation in terrorist activity. Each of the five core terrorist uses of the Internet is explained and analyzed in more detail below.

Five Terrorist Uses of the Net

Information Provision

This refers to efforts by terrorists to engage in publicity, propaganda and, ultimately, psychological warfare. The Internet, and the advent of the World Wide Web in particular, have significantly increased the opportunities for terrorists to secure publicity. This can take the form of historical information, profiles of leaders, manifestos, etc. But terrorists can also use the Internet as a tool of psychological warfare through spreading disinformation, delivering threats, and disseminating horrific images, such as the beheading of American entrepreneur Nick Berg in Iraq and US journalist

Daniel Pearl in Pakistan via their Web sites.[15] These functions are clearly improved by the Web's enhanced volume, increased speed of data transmission, low-cost, relatively uncontrolled nature, and global reach.

Until the advent of the Internet, terrorists' hopes of winning publicity for their causes and activities depended on attracting the attention of television, radio, or the print media. As Weimann points out, "these traditional media have 'selection thresholds' (multistage processes of editorial selection) that terrorists often cannot reach." [16] The same criteria do not, of course, apply to the terrorists' own websites. The Internet thus offers terrorist groups an unprecedented level of direct control over the content of their message(s). It considerably extends their ability to shape how different target audiences perceive them and to manipulate not only their own image, but also the image of their enemies. Although, for many groups, their target audience may be small, an Internet presence is nonetheless expected. Regardless of the number of hits a site receives, a well-designed and well-maintained Web site gives a group an aura of legitimacy.

Financing

This refers to efforts by terrorist groups to raise funds for their activities. Money is terrorism's lifeline; it is "the engine of the armed struggle." [17] The immediacy and interactive nature of Internet communication, combined with its high-reach properties, opens up a huge potential for increased financial donations as has been demonstrated by a host of non-violent political organizations and civil society actors. Terrorists seek financing both via their Web sites and by using the Internet infrastructure to engage in resource mobilization using illegal means.

Direct Solicitation via Terrorist Web Sites

Numerous terrorist groups request funds directly from Web surfers who visit their sites. Such requests may take the form of general statements underlining the organizations need for money, more often than not however requests are more direct urging supporters to donate immediately and supplying either bank account details or an Internet payment option. For example, the IRA's main Web site contains a page on which visitors can make credit card donations.[18] While, at one time, the Ulster Loyalist Information Service, which was affiliated with the Loyalist Volunteer Force (LVF), and accepted funds via PayPal, invited those who were "uncomfortable with making monetary donations" to donate other items, including bullet-proof vests. A second, and related, fundraising method is to profile site visitors by employing user demographics (yielded, for example, from identifying information entered in online questionnaires or order forms) and to contact those whose profiles indicate they are potential financial supporters, a function which may be carried out by proxies, ac-

cording to Tibbetts.[19] A third way in which groups raise funds is through the establishment of online stores and the sale of items such as books, audio and video tapes, flags, t-shirts, etc.

Exploitation of e-Commerce Tools & Entities

The Internet facilitates terrorist financing in a number of other ways besides direct solicitation via terrorist Web sites. According to Jean-Francois Ricard, one of France's top anti-terrorism investigators, many Islamist terror plots are financed through credit card fraud.[20] Imam Samudra, sentenced to death for his part in the Bali bombing of 2002, has published a prison memoir of some 280 pages, which includes a paper that acts as a primer on 'carding.' [21]

According to Dutch experts, there is strong evidence from international law enforcement agencies such as the FBI that at least some terrorist groups are financing their activities via advanced fee fraud, such as Nigerian-style scam e-mails. To date, however, solid evidence for such claims has not entered the public realm.[22] There is ample evidence, however, to support the contention that terrorist-affiliated entities and individuals have established Internet-related front businesses as a means of raising money to support their activities. For example, in December 2002, InfoCom, a Texas-based ISP, was indicted along with its individual corporate officers on thirty-three counts relating to its provision of communication services, in-kind support, and funds to terrorist organizations including Hamas and its affiliate the Holy Land Foundation for Relief and Development (HLFRD). InfoCom's capital was donated primarily by Nadia Elashi Marzook, wife of Hamas figurehead Mousa Abu Marzook.[23]

Exploitation of Charities and Fronts

Terrorist organizations have a history of exploiting not just businesses, but also charities as undercover fundraising vehicles. This is particularly popular with Islamist terrorist groups, probably because of the injunction that observant Muslims make regular charitable donations. In some cases, terrorist organizations have actually established charities with allegedly humanitarian purposes. Examples of such undertakings include Mercy International, Wafa al-Igatha al-Islamiya, Rabita Trust, Al Rasheed Trust, Global Relief Fund, Benevolence International Foundation, and Help The Needy. Along with advertising in sympathetic communities' press, these 'charities' also advertised on websites and chat rooms with Islamic themes, pointing interested parties to their Internet homepages.

Terrorists have also infiltrated branches of existing charities to raise funds clandestinely. Many such organizations provide the humanitarian services advertised: feeding, clothing, and educating the poor and illiterate, and providing medical care for the sick. However, some such organizations, in addition to pursuing their publicly stated

mission of providing humanitarian aid, also pursue a covert agenda of providing material support to militant groups. These organizations' Web-based publicity materials may or may not provide hints as to their secret purposes.

As the LVF and InfoCom examples show, the support sought by and provided to terrorist organizations may not always be in the form of cash. Terrorist groups use the Internet to solicit other fungible goods, to accumulate supplies, and to recruit foot soldiers. In this paper, however, the term 'financing' has been used in its narrow sense to mean the remittance of money. Nonetheless, it may also be used as shorthand for the accumulation of any of the material resources necessary for terrorists to maintain their organizations and carry out operations.

Networking

This refers to groups' efforts to flatten their organizational structures and act in a more decentralized manner through the use of the Internet, which allows dispersed actors to communicate quickly and coordinate effectively at low cost. The Internet allows not only for intra-group communication, but also inter-group connections. The Web enhances terrorists' capacities to transform their structures and build these links because of the alternative space it provides for communication and discussion and the hypertext nature of the Web, which allows for groups to link to their internal subgroups and external organizations around the globe from their central Web site.

Transforming Organizational Structures [24]

Rand's John Arquilla, David Ronfeldt, and Michele Zanini have been pointing to the emergence of new forms of terrorist organization attuned to the information age for some time. They contend, "Terrorists will continue to move from hierarchical toward information-age network designs. More effort will go into building arrays of transnationally internetted groups than into building stand alone groups." [25] This type of organizational structure is qualitatively different from traditional hierarchical designs. Terrorists are ever more likely to be organized to act in a more fully networked, decentralized, 'all-channel' manner. Ideally, there is no single, central leadership, command, or headquarters. Within the network as a whole there is little or no hierarchy and there may be multiple leaders depending upon the size of the group. In other words, there is no specific heart or head that can be targeted. To realize its potential, such a network must utilize the latest information and communications technologies. The Internet is becoming an integral component of such organizations, according to the Rand analysts.[26]

Planning and Coordination

"Many terrorist groups share a common goal with mainstream organizations and institutions: the search for greater efficiency through the Internet." [27] Several reasons have been put forward to explain why modern IT systems, especially the Internet, are so useful for terrorists in establishing and maintaining networks. As already discussed, new technologies enable quicker, cheaper, and more secure information flows. In addition, the integration of computing with communications has substantially increased the variety and complexity of the information that can be shared.[28]

This led Michele Zanini to hypothesize that "the greater the degree of organizational networking in a terrorist group, the higher the likelihood that IT is used to support the network's decision making." [29] Zanini's hypothesis appears to be borne out by recent events. For example, many of the terrorists indicted by the United States government since 9/11 communicated via e-mail. The indictment of four members of the Armed Islamic Group (Gama'a al-Islamiyya) alleges that computers were used "to transmit, pass and disseminate messages, communications and information between and among IG leaders and members in the United States and elsewhere around the world." [30] Similarly, six individuals indicted in Oregon in 2002 allegedly communicated via e-mail regarding their efforts to travel to Afghanistan to aid Al-Qaeda and the Taliban in their fight against the United States.[31,32]

The Internet has the ability to connect not only members of the same terrorist organizations but also members of different groups. For example, hundreds of so-called 'jihadist' sites exist that express support for terrorism. According to Weimann, these sites and related forums permit terrorists in places as far-flung as Chechnya, Palestine, Indonesia, Afghanistan, Turkey, Iraq, Malaysia, the Philippines, and Lebanon to exchange not only ideas and suggestions, but also practical information about how to build bombs, establish terror cells, and ultimately perpetrate attacks.[33]

Mitigation of Risk

As terrorist groups come under increasing pressure from law enforcement, they have been forced to evolve and become more decentralized. This is a structure to which the Internet is perfectly suited. The Net offers a way for like-minded people located in different communities to interact easily, which is particularly important when operatives may be isolated and having to 'lie low.' Denied a physical place to meet and organize, many terrorist groups are alleged to have created virtual communities through chat rooms and Web sites in order to continue spreading their propaganda, teaching, and training. Clearly, "information technology gives terrorist organizations global power and reach without necessarily compromising their invisibility." [34] It "puts distance between those planning the attack and their targets…[and] provides terrorists a place to plan without the risks normally associated with cell or satellite phones." [35]

Recruitment

This refers to groups' efforts to recruit and mobilize sympathizers to more actively support terrorist causes or activities. The Web offers a number of ways for achieving this: it makes information gathering easier for potential recruits by offering more information, more quickly, and in multimedia format; the global reach of the Web allows groups to publicize events to more people; and by increasing the possibilities for interactive communication, new opportunities for assisting groups are offered, along with more chances for contacting the group directly. Finally, through the use of discussion forums, it is also possible for members of the public—whether supporters or detractors of a group—to engage in debate with one another. This may assist the terrorist group in adjusting their position and tactics and, potentially, increasing their levels of support and general appeal.[36]

Online recruitment by terrorist organizations is said to be widespread. Fritz, Harris, Kolb, Larich, and Stocker provide the example of an Iranian site that boasts an application for suicide bombers guaranteeing that the new 'martyr' will take seventy relatives with him into heaven. If the recruit is unsure about joining, or if the group is unsure about the recruit, he is directed to a chat room where he is 'virtually' vetted. If he passes muster, he will be directed to another chat room for further vetting, and finally contacted personally by a group member. This process is said to be aimed at weeding out 'undesirables' and potential infiltrators.[37] It is more typical, however, for terrorist groups to actively solicit for recruits rather than waiting for them to simply present themselves. Weimann suggests that terrorist recruiters may use interactive Internet technology to roam online chat rooms looking for receptive members of the public, particularly young people. Electronic bulletin boards could also serve as vehicles for reaching out to potential recruits.[38]

Information Gathering

This refers to the capacity of Internet users to access huge volumes of information, which was previously extremely difficult to retrieve as a result of its being stored in widely differing formats and locations. Today, there are literally hundreds of Internet tools that aid in information gathering; these include a range of search engines, millions of subject-specific email distribution lists, and an almost limitless selection of esoteric chat and discussion groups. One of the major uses of the Internet by terrorist organizations is thought to be information gathering. Unlike the other uses mentioned above terrorists' information gathering activities rely not on the operation of their own Web sites, but on the information contributed by others to "the vast digital library" that is the Internet.[39] There are two major issues to be addressed here. The first may be termed 'data mining' and refers to terrorists using the Internet to collect and assemble information about specific targeting opportunities. The second issue is 'in-

formation sharing,' which refers to more general online information collection by terrorists.

Data Mining

In January 2003, U.S. Defence Secretary Donald Rumsfeld warned in a directive sent to military units that too much unclassified, but potentially harmful material was appearing on Department of Defence (DoD) Web sites. Rumsfeld reminded military personnel that an Al-Qaeda training manual recovered in Afghanistan states: "Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty percent of information about the enemy." He went on to say, "at more than 700 gigabytes, the DoD Web-based data makes a vast, readily available source of information on DoD plans, programs and activities. One must conclude our enemies access DoD Web sites on a regular basis." [40]

In addition to information provided by and about the armed forces, the free availability of information on the Internet about the location and operation of nuclear reactors and related facilities was of particular concern to public officials post 9/11. Roy Zimmerman, director of the Nuclear Regulatory Commission's (NRC) Office of Nuclear Security and Incident Response, said the 9/11 attacks highlighted the need to safeguard sensitive information. In the days immediately after the attacks, the NRC took their Web site entirely off line. When it was restored weeks later, it had been purged of more than 1,000 sensitive documents. Initially, the agency decided to withhold documents if "the release would provide clear and significant benefit to a terrorist in planning an attack." Later, the NRC tightened the restriction, opting to exclude information "that could be useful or could reasonably be useful to a terrorist." According to Zimmerman, "it is currently unlikely that the information on our Web site would provide significant advantage to assist a terrorist." [41]

The measures taken by the NRC were not exceptional. According to a report produced by OMB Watch,[42] since 9/11 thousands of documents and tremendous amounts of data have been removed from U.S. government sites. The difficulty, however, is that much of the same information remains available on private sector Web sites.[43] Patrick Tibbetts points to the Animated Software Company's Web site which has off-topic documents containing locations, status, security procedures and other technical information concerning dozens of U.S. nuclear reactors,[44] while the Virtual Nuclear Tourist site contains similar information. The latter site is particularly detailed on specific security measures that may be implemented at various nuclear plants worldwide.[45,46]

Many people view such information as a potential gold mine for terrorists. Their fears appear well founded given the capture of Al-Qaeda computer expert Muhammad Naeem Noor Khan in Pakistan in July 2004, which yielded a computer filled with

photographs and floor diagrams of buildings in the U.S. that terrorists may have been planning to attack.[47] The Australian press has also reported that a man charged with terrorism offences there had used Australian government Web sites to get maps, data, and satellite images of potential targets. The government of New South Wales was said to be considering restricting the range of information available on their Web sites as a result.[48]

Terrorists can also use the Internet to learn about antiterrorism measures. Gabriel Weimann suggests that a simple strategy like conducting word searches of online newspapers and journals could allow a terrorist to study the means designed to counter attacks, or the vulnerabilities of these measures.[49]

Sharing Information

Policymakers, law enforcement agencies, and others are also concerned about the proliferation of 'how to' Web pages devoted to explaining, for example, the technical intricacies of making homemade bombs. Many such devices may be constructed using lethal combinations of otherwise innocuous materials; today, there are hundreds of freely available online manuals containing such information. As early as April 1997, the U.S. Department of Justice had concluded that the availability of this information played a significant role in facilitating terrorist and other criminal acts.[50]

As an example, Jessica Stern points to *Bacteriological Warfare: A Major Threat to North America* (1995), which is described on the Internet as a book for helping readers survive a biological weapons attack and is subtitled 'What Your Family Can Do Before and After.' However, it also describes the reproduction and growth of biological agents and includes a chapter entitled 'Bacteria Likely to Be Used by the Terrorist.' The text is available for download, in various edited and condensed formats, from a number of sites while hard copies of the book are available for purchase over the Internet from sites such as Barnesandnoble.com for as little as $13.[51]

More recently, an Al-Qaeda laptop found in Afghanistan had been used to visit the Web site of the French Anonymous Society (FAS) on several occasions. The FAS site publishes a two-volume *Sabotage Handbook* that contains sections on planning an assassination and anti-surveillance methods amongst others.[52] A much larger manual, nicknamed *The Encyclopedia of Jihad* and prepared by Al Qaeda, runs to thousands of pages; distributed via the Web, it offers detailed instructions on how to establish an underground organization and execute terror attacks.[53]

This kind of information is sought out not just by sophisticated terrorist organizations but also by disaffected individuals prepared to use terrorist tactics to advance their idiosyncratic agendas. In 1999, for instance, right-wing extremist David Copeland planted nail bombs in three different areas of London: multiracial Brixton, the largely

Bangladeshi community of Brick Lane, and the gay quarter in Soho. Over the course of three weeks, he killed three people and injured 139. At his trial, he revealed that he had learned his deadly techniques from the Internet by downloading copies of *The Terrorist's Handbook* and *How to Make Bombs: Book Two*. Both titles are still easily accessible.[54]

The Open Source Threat?

The threat posed by the easy availability of bomb-making and other 'dangerous information' is a source of heated debate. Patrick Tibbetts warns against underestimating the feasibility of such threats. He points out that captured Al Qaeda materials include not only information compiled on 'home-grown explosives,' but also indicate that this group are actively pursuing data and technical expertise necessary to pursue CBRN weapons programs. According to Ken Katzman, a terrorism analyst for the Congressional Research Service, much of the material in these captured documents was probably downloaded from the Internet.[55] As a result, many have called for laws restricting the publication of bomb-making instructions on the Internet, while others have pointed out that this material is already easily accessible in bookstores and libraries.[56] In fact, much of this information has been available in print media since at least the late 1960s, with the publication of William Powell's *The Anarchist Cookbook* and other, similar titles.

Jessica Stern has observed: "In 1982, the year of the first widely reported incident of tampering with pharmaceuticals, the Tylenol case, only a few poisoning manuals were available, and they were relatively hard to find." [57] This is doubtless true; they were hard to find, but they were available. As Stern herself concedes, currently how-to manuals on producing chemical and biological agents are not just available on the Internet, but are advertised in paramilitary journals sold in magazine shops all over the United States.[58] According to a U.S. government report, over fifty publications describing the fabrication of explosives and destructive devices are listed in the Library of Congress and are available to any member of the public, as well as being easily available commercially.[59,60] Ken Shirriff sums up this point well:

> Note that *The Anarchist Cookbook* is available from nearly any bookstore in the U.S. These dangerous institutions will also sell you Nazi and hate literature, pornography, instructions on growing drugs, and so forth. For some reason, getting this stuff from a bookstore is not news, but getting it over the Internet is.[61]

Despite assertions to the contrary,[62] the infamous *Anarchist Cookbook* [63] is not available online, although it is easily purchased from bookstores or from Amazon.com. The anonymous authors of Web sites claiming to post the *Cookbook* and similar texts often include a disclaimer that the processes described should not be carried out. This is because many of the 'recipes' have a poor reputation for reliability and safety.

Perhaps the most likely 'recipes' to be of use to terrorists are those related to hacking tools and activities. Such information is also likely to be considerably more accurate than bomb making information, for example; this is because the Internet is both the domain and tool of hackers. In testimony before the U.S. House Armed Services Committee in 2003, Purdue University professor and information assurance expert, Eugene Spafford said bulletin boards and discussion lists teach hacking techniques to anyone: "We have perhaps a virtual worldwide training camp," he testified.[64] Terrorists have been known to exploit this resource. Imam Samudra's instructions regarding the use of chat rooms favored by hackers to obtain information about 'carding' have already been mentioned. In 1998, Khalid Ibrahim, who identified himself as an Indian national, sought classified and unclassified U.S. government software and information, as well as data from India's Bhabha Atomic Research Center, from hackers communicating via Internet Relay Chat (IRC). Using the online aliases RahulB and Rama3456, Ibrahim began frequenting online cracker hangouts in June 1998. In conversations taken from IRC logs, Ibrahim claimed to be a member of Harkat-ul-Ansar, a militant Kashmiri separatist group.[65]

Finally, it is important to keep in mind that removal of technical information from public Web sites is no guarantee of safeguarding it. In essence, this effort is akin to 'closing the barn door after the horse has bolted.' Intelligence and technical data obtained by terrorist operatives prior to 9/11 can be archived, stored and distributed surreptitiously irrespective of government or private attempts to squelch its presence on the Internet in 2005. Indeed, these materials can be loaded onto offshore or other international Web servers that cannot be affected by U.S. legislation, rendering any attempt to halt their spread outside the reach of American law enforcement.[66]

Fighting Back

Use of the Internet is a double-edged sword for terrorists. They are not the only groups 'operating' the Net,[67] which can act as a valuable instrumental power source for anti-terrorist forces also. The more terrorist groups use the Internet to move information, money, and recruits around the globe, the more data that is available with which to trail them. Since 9/11 a number of groups have undertaken initiatives to disrupt terrorist use of the Internet, although a small number of such efforts were also undertaken previous to the attacks. Law enforcement agencies have been the chief instigators of such initiatives, but they have been joined in their endeavors by other government agencies as well as concerned individuals and various groups of hacktivists.

The Role of Law Enforcement and Intelligence Agencies

Intelligence Gathering

The bulk of this paper has been concerned with showing how the Internet can act as a significant source of instrumental power for terrorist groups. Use of the Internet can nonetheless also result in significant undesirable effects for the same groups. First, unless terrorists are extremely careful in their use of the Internet for e-mail communication, general information provision, and other activities, they may unwittingly supply law enforcement agencies with a path direct to their door. Second, by putting their positions and ideological beliefs in the public domain, terrorist groups invite opposing sides to respond to these. The ensuing war of words may rebound on the terrorists as adherents and potential recruits are drawn away.[68] Perhaps most importantly, however, the Internet and terrorist Web sites can serve as a provider of open source intelligence for states' intelligence agencies. Although spy agencies are loathe to publicly admit it, it is generally agreed that the Web is playing an ever-growing role in the spy business.

According to the 9/11 Commission's *Staff Statement No. 11*, "open sources—the systematic collection of foreign media—has always been a bedrock source of information for intelligence. Open source remains important, including among terrorist groups that use the media and the Internet to communicate leadership guidance." [69] By the 1990s the US government's Foreign Broadcast Information Service (FBIS) had built a significant translation effort as regards terrorism-related media. Thus many now believe that terrorists' presence on the Internet actually works against them. "A lot of what we know about Al-Qaida is gleaned from [their] websites," according to Steven Aftergood, a scientist at the Federation of American Scientists in Washington, D.C., and director of the non-profit organization's Project on Government Secrecy.[70] "They are a greater value as an intelligence source than if they were to disappear" (as quoted by Lasker).[71] For example, Web sites and message boards have been known to function as a kind of early warning system. Two days before the 9/11 attacks, a message appeared on the popular Dubai-based Alsaha.com discussion forum proclaiming that "in the next two days," "a big surprise" would come from the Saudi Arabian region of Asir. The remote province adjacent to Yemen was where most of the nineteen hijackers hailed from.[72]

Innovations such as the FBIS, while useful, do not tell the whole story, however. The problem begins with the sheer volume of information floating about in cyberspace. According to the 9/11 Commission's *Staff Statement No. 9*, prior to 9/11 the FBI did not have a sufficient number of translators proficient in Arabic and other relevant languages, which by early 2001 had resulted in a significant backlog of untranslated intelligence intercepts. In addition, prior to 9/11, the FBI's investigative activities were governed by Attorney General Guidelines, first put in place in 1976 and revised

in 1995, to guard against the misuse of government power. The Guidelines limited the investigative methods and techniques available to FBI agents conducting preliminary investigations of potential terrorist activities. In particular, they prohibited the use of publicly available source information, such as that found on the Internet, unless specified criteria were present.[73] These guidelines have since been modified and terrorist Web sites are thought to be under increased surveillance since 9/11, especially by Western intelligence agencies.[74] This task remains gargantuan, however; information gleaned from the Net must be corroborated and verified before it can be added to the intelligence mix. This requires significant input of operatives and resources. And still intelligence agencies simply cannot monitor the entire Internet all of the time.

Technological Fixes

Given the above, it is unsurprising that many U.S. officials and commentators are recommending that any additional funds that become available to the intelligence agencies be spent on human intelligence capabilities, rather than new technology. Others, however, are convinced that new technologies need to be developed and deployed in the fight against terrorism. They bemoan the fact that prior to 9/11, "Signals intelligence collection against terrorism, while significant, did not have sufficient funding within the NSA. The NSA's slow transformation meant it could not keep pace with advances in telecommunications." [75] Although DCS-1000—more commonly known as Carnivore—the FBI's e-mail packet-sniffer system has not been employed since 2002, Bureau officials have instead employed commercially available monitoring applications to aid in their investigations. Intelligence agencies are also said to be deploying the classic spy tactic of establishing so-called 'honey pots' with a high-tech twist: in this case, setting up bogus Web sites to attract those people they are seeking to monitor.[76] Numerous other technological fixes are also in the works.

Other Innovations

It should be clear at this stage that the events of 9/11 impacted intelligence and law enforcement agencies not just in the United States, but around the world. On this side of the Atlantic, MI5 took the unprecedented step of posting an appeal for information about potential terrorists on dissident Arab websites. The message, in Arabic, was placed on sites that the authorities knew were accessed by extremists, including 'Islah.org,' a Saudi Arabian opposition site, and 'Qoqaz.com,' a Chechen site which advocated *jihad*. The message read:

> The atrocities that took place in the USA on 11 September led to the deaths of about five thousand people, including a large number of Muslims and people of other faiths. MI5 (the British Security Service) is responsible for countering terrorism to protect all UK citizens of whatever faith or ethnic group. If you think you can help us to prevent future outrages call us in confidence on 020-7930 9000.

MI5 were hopeful of eliciting information from persons on the margins of extremist groups or communities who were sufficiently shocked by the events of 9/11 to want to contact the agency. The agency had intended to post the message on a further fifteen sites known to be accessed by radicals, but many of these were shut down by the FBI in the aftermath of the attacks.[77] The events of 9/11 prompted numerous states' intelligence agencies to reappraise their online presence. Since 2001, MI5 has substantially enhanced its Web site while in 2004, Israel's Mossad spy agency launched a Web site aimed at recruiting staff.

Other Agencies: Sanitising Government Sites

U.S. government Web sites were vital repositories of information for Internet users in the days and weeks following the 9/11 attacks. The sites became important venues for those both directly and indirectly affected by the events of 9/11, members of the public wishing to donate to the relief efforts, and the various agencies' own employees, some of whom were victims of the attacks (or later of the anthrax scares).[78]

While some agencies were uploading information onto the Net, however, others were busy erasing information from their sites. To avoid providing information that might be useful to terrorists planning further attacks, federal agencies, as well as some state and private Web page operators, took large amounts of material off the Internet in the wake of the 9/11 attacks. Some of the erasures were voluntary; others were carried out following requests from U.S. government departments. As mentioned earlier the Nuclear Regulatory Commission, which regulates American nuclear power plants, closed its Web site down for a period following a request from the Department of Defence that it do so. Although no other agency removed its entire site, pages were erased from the Web sites of the Department of Energy, the Interior Department's Geological Survey, the Federal Energy Regulatory Commission, the Environmental Protection Agency, the Federal Aviation Administration, the Department of Transportation's Office of Pipeline Safety, the National Archives and Records Administration, the NASA Glenn Research Centre, the International Nuclear Safety Centre, the Los Alamos National Laboratory, the Bureau of Transportation Statistics' Geographic Information Service, and the National Imagery and Mapping Agency.[79]

What sorts of information was removed from the sites? The Environmental Protection Agency (EPA) removed thousands of chemical industry risk management plans dealing with hazardous chemical plants from its site. Department of Transportation officials removed pipeline mapping information as well as a study describing risk profiles of various chemicals, while the Bureau of Transportation Statistics removed the National Transportation Atlas Databases and the North American Transportation Atlas, which environmentalists had used to assess the impact of transportation proposals. The Center for Disease Control and Prevention removed a *Report on Chemical Ter-*

rorism that described industry's shortcomings in preparing for a possible terrorist attack.[80] Many of the agencies posted notices that the information had been removed because of its possible usefulness to terrorists.

Hackers and Hacktivists

Hackers also took to the Net in the aftermath of the terror attacks, some to voice their rage, others to applaud the attackers. A group calling themselves the Dispatchers proclaimed that they would destroy Web servers and Internet access in Afghanistan and also target nations that support terrorism. The group proceeded to deface hundreds of Web sites and launch Distributed Denial of Service (DoS) attacks against targets ranging from the Iranian Ministry of the Interior to the Presidential Palace of Afghanistan. Another group, known as Young Intelligent Hackers Against Terror (YIHAT) claimed, in mid-October 2001, to be negotiating with one European and one Asian government to 'legalize' the groups hacking activities in those states. The group's founder, Kim Schmitz, claimed the group breached the systems of two Arabic banks with ties to Osama Bin Laden, although a spokesperson for the bank denied any penetration had occurred. The group, whose stated mission is to impede the flow of money to terrorists, issued a statement on their Web site requesting that corporations make their networks available to group members for the purpose of providing the "electronic equivalent to terrorist training camps." Later, their public Web site was taken offline, apparently in response to attacks from other hackers.[81]

Not all hacking groups were supportive of the so-called 'hacking war.' On 14 September 2001, the Chaos Computer Club, an organization of German hackers, called for an end to the protests and for all hackers to cease vigilante actions. They called instead for global communication to resolve the conflict: "we believe in the power of communication, a power that has always prevailed in the end and is a more positive force than hatred" (as quoted by Hauss and Samuel).[82] A well-known group of computer enthusiasts, known as Cyber Angels, who promote responsible behaviour, also spoke out against the hacking war. They sponsored television advertisements in the US urging hackers to help gather information and intelligence on those who were participating in this hacktivism.[83] In any event, the predicted escalation in hack attacks [84] did not materialize. In the weeks following the attacks, Web page defacements were well publicized, but the overall number and sophistication of these remained rather low. One possible reason for the non-escalation of attacks could be that many hackers—particularly those located in the U.S.—were wary of being negatively associated with the events of 9/11 and curbed their activities as a result.

Since 9/11 a number of Web-based organisations have been established to monitor terrorist Web sites. One of the most well-known of such sites is Internet Haganah,[85] self-described as "an internet counterinsurgency." Also prominent is the Washington

DC-based Search for International Terrorist Entities (SITE) Institute [86] that, like Internet Haganah, focuses on Islamic terror groups. Clients of SITE's fee-based intelligence service are said to include the FBI, Office of Homeland Security, and various media organizations. SITE's co-founder and director, Rita Katz, has commented: "It is actually to our benefit to have some of these terror sites up and running by American companies. If the servers are in the US, this is to our advantage when it comes to monitoring activities" (as quoted by Lasker).[87] Aaron Weisburd, who runs Internet Haganah out of his home in Southern Illinois, says his goal is to keep the extremists moving from address to address: "The object isn't to silence them –the object is to keep them moving, keep them talking, force them to make mistakes, so we can gather as much information about them as we can, each step of the way" (as quoted by Lasker).[88]

Conclusion

Researchers are still unclear whether the ability to communicate online worldwide has resulted in an increase or a decrease in terrorist acts. It is agreed, however, that online activities substantially improve the ability of such terrorist groups to raise funds, lure new faithful, and reach a mass audience.[89] The most popular terrorist sites draw tens of thousands of visitors each month. Obviously, the Internet is not the only tool that a terrorist group needs to 'succeed.' However, the Net can add new dimensions to existing assets that groups can utilize to achieve their goals as well as providing new and innovative avenues for expression, fundraising, recruitment, etc. At the same time, there are also tradeoffs to be made. High levels of visibility increase levels of vulnerability, both to scrutiny and security breaches. The proliferation of official terrorist sites appears to indicate that the payoffs, in terms of publicity and propaganda value, are understood by many groups to be worth the risks.

Notes:

[1] As quoted in New 2004. Clarke was the White House cyber security chief during the tenures of both Bill Clinton and George W. Bush. He resigned in January 2003.

[2] David Resnick, "Politics on the Internet: The Normalization of Cyberspace," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York & London: Routledge, 1999), 55-56.

[3] Wayne Rash, *Politics on the Nets: Wiring the Political Process* (New York: W.H. Freeman, 1997), 176-177.

[4] Steve Furnell and Matthew Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium," *Computers and Security* 18, no. 1 (1999): 30-32.

[5] Fred Cohen, "Terrorism and Cyberspace," *Network Security* 5 (2002): 18-19.

[6] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" *Parameters* (Spring 2003): 114-122, <http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.htm> (12 Dec. 2005).

[7] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" 113.

[8] Gabriel Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet* (Washington DC: United States Institute of Peace, 2004), <http://www.usip.org/pubs/specialreports/sr116.pdf> (12 Dec. 2005), 5-11.

[9] Such overlaps are not just evident amongst those who adopt a use paradigm, but are shared with those who adopt an Information Operations (IO) approach (see Dorothy Denning, "Information Operations and Terrorism," 2004 (Pre-Print); N.E. Emery, R. S. Earl, and R. Buettner, "Terrorist Use of Information Operations," *Journal of Information Warfare* 3, no. 2 (2004); Kevin O'Brien and Izhar Lev, "Information Operations and Counterterrorism," *Jane's Intelligence Review* 14, no. 9 (2002).

[10] Furnell and Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium."

[11] Cohen, "Terrorism and Cyberspace."

[12] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning.'"

[13] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*.

[14] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning;'" Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*.

[15] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 5.

[16] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 6.

[17] Loretta Napoleoni, "Money and Terrorism," *Strategic Insights* 3, no. 4 (2004): 1, <http://www.ciaonet.org/olj/si/si_3_4/si_3_4_nal01.pdf> (12 Dec. 2005).

[18] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 7.

[19] Patrick S. Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," Unpublished Paper (Fort Leavenworth, Kansas: United States Army Command and General Staff College, 2002), 20, <http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=0&keyfieldvalue=ADA403802&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA403802.pdf> (15 May 2005).

[20] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" 117.

[21] Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War into Cyberspace," *Washington Post*, 14 December 2004, A19, <http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html> (12 Dec. 2005).

[22] Jan Libbenga, "Terrorists Grow Fat on E-Mail Scams," *The Register*, 28 September 2004, <http://www.theregister.co.uk/2004/09/28/terrorist_email_scams/> (12 Dec. 2005).

[23] Todd M. Hinnen, "The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet," *Columbia Science and Technology Law Review* 5 (2004): 18, <http://www.stlr.org/html/volume5/hinnenintro.html> (12 Dec. 2005); see also Steven Emerson, "Fund-Raising Methods and Procedures for International T`errorist

Organizations," Testimony before the House Committee on Financial Services, 12 February 2002, 11-12, 16, <http://financialservices.house.gov/media/pdf/021202se.pdf> (12 Dec. 2005).

[24] For a brief introduction to organizational network analysis, see John Arquilla and David Ronfeldt, "Networks, Netwars and the Fight for the Future," *First Monday* 6, no. 10 (2001), <http://www.firstmonday.org/issues/issue6_10/ronfeldt/index.html> (12 Dec. 2005); John Arquilla and David Ronfeldt, "What Next for Networks and Netwars?" in *Networks and Netwars*, ed. John Arquilla and David Ronfledt (California: Rand, 2001), 319-323, <http://www.rand.org/publications/MR/MR1382/MR1382.ch10.pdf> (12 Dec. 2005).

[25] John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar and Information-Age Terrorism," in *Countering the New Terrorism*, ed. Ian O. Lesser, Bruce Hoffman, John Arquilla, David F. Ronfeldt, Michele Zanini, and Brian Michael Jenkins (Santa Monica, Calif.: Rand, 1999), 41, <www.rand.org/publications/MR/MR989/MR989.chap3.pdf> (12 Dec. 2005).

[26] Arquilla, Ronfeldt, and Zanini, "Networks, Netwar and Information-Age Terrorism," 48-53; John Arquilla, and David Ronfeldt, "Emergence and Influence of the Zapatista Social Netwar," in *Networks and Netwars*, ed. John Arquilla and David Ronfeldt (California: Rand, 2001), <http://www.rand.org/publications/MR/MR1382/MR1382.ch6.pdf> (12 Dec. 2005).

[27] Peter Margulies, "The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment," *UCLA Journal of Law and Technology* 8, no. 2 (2004): 2, <http://www.lawtechjournal.com/articles/2004/04_041207_margulies.pdf> (12 Dec. 2005).

[28] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 9.

[29] Michele Zanini, "Middle Eastern Terrorism and Netwar," *Studies in Conflict and Terrorism* 22, no. 3 (1999): 251.

[30] Indictment, United States v. Sattar, No. 02-CRIM-395, 11 (S.D.N.Y Apr. 9, 2002). Available online at <http://news.findlaw.com/hdocs/docs/terrorism/ussattar040902ind.pdf> (12 Dec. 2005).

[31] Hinnen, "The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet," 38.

[32] Indictment, United States v. Battle, No. CR 02-399 HA, 5 (D.Or. Oct. 2, 2002). Available online at <http://news.findlaw.com/hdocs/docs/terrorism/usbattle100302ind.pdf> (12 Dec. 2005).

[33] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 9.

[34] Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," 5.

[35] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" 119.

[36] Rachel Gibson and Stephen Ward, "A Proposed Methodology for Studying the Function and Effectiveness of Party and Candidate Web Sites," *Social Science Computer Review* 18, no. 3 (2000): 305-306; Kevin Soo Hoo, Seymour Goodman, and Lawrence Greenberg, "Information Technology and the Terrorist Threat," *Survival* 39, no. 3 (1997): 140; Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 8.

[37] Kathryn Fritz, Lindsay Harris, Daniel Kolb, Paula Larich, and Kathleen Stocker, "Terrorist Use of the Internet and National Response," Unpublished Paper (College Park: University of Maryland, 2004), 9, <http://www.wam.umd.edu/~larich/735/index.html> (12 Dec. 2005)

[38] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 8.

[39] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 6.

[40] Declan McCullagh, "Military Worried about Web Leaks," *C|Net News*, 16 January 2003, <http://news.com.com/2100-1023-981057.html> (12 Dec. 2005).

[41] Mike M. Ahlers, "Blueprints for Terrorists?" *CNN.com*, 19 November 2004, <http://www.cnn.com/2004/US/10/19/terror.nrc/> (12 Dec. 2005).

[42] OMB Watch is a watchdog group based in Washington DC. Their home page is at <http://www.ombwatch.org> (12 Dec. 2005).

[43] McCullagh, "Military Worried about Web Leaks;" Gary D. Bass and Sean Moulton, "The Bush Administration's Secrecy Policy: A Call to Action to Protect Democratic Values," Working Paper (Washington DC: OMB Watch, 2002), <http://www.ombwatch.org/rtk/secrecy.pdf> (12 Dec. 2005).

[44] See <http://www.animatedsoftware.com/environm/no_nukes/nukelist1.htm>.

[45] See <http://www.nucleartourist.com/>.

[46] Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," 15.

[47] Douglas Jehl and David Johnston, "Reports That Led to Terror Alert Were Years Old, Officials Say," *New York Times*, 3 August 2004; Dan Verton and Lucas Mearian, "Online Data a Gold Mine for Terrorists," *ComputerWorld*, 6 August 2004, <http://www.computerworld.com/securitytopics/security/story/0,10801,95098,00.html> (12 Dec. 2005).

[48] Australian Broadcasting Corporation (ABC), "NSW Considers Limits on Government Website," *ABC Online*, 28 April 2004.

[49] Gabriel Weimann, "Terror on the Internet: The New Arena, The New Challenges" (paper presented at the International Studies Association (ISA) Annual Conference, Montreal, Quebec, Canada, 17-20 March 2004), 15.

[50] US Department of Justice, *Report on the Availability of Bombmaking Information, the Extent to Which Its Dissemination Is Controlled by Federal Law, and the Extent to Which Such Dissemination May Be Subject to Regulation Consistent with the First Amendment to the United States Constitution* (Washington DC: US Department of Justice, 1997), 15-16, <http://cryptome.org/abi.htm> (12 Dec. 2005).

[51] Jessica Stern, *The Ultimate Terrorists* (Cambridge, MA: Harvard University Press, 1999), 51.

[52] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" 115; Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 9.

[53] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 9.

[54] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 10.

[55] Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," 17.

[56] Anti-Defamation League, "Terrorist Activities on the Internet," *Terrorism Update* (Winter 1998), <http://www.adl.org/Terror/focus/16_focus_a.asp> (12 Dec. 2005).

[57] Stern, *The Ultimate Terrorists*, 50.

[58] Stern, *The Ultimate Terrorists*, 51.

[59] The same report mentions that one Kansas bomber got his bomb instructions from the August 1993 *Reader's Digest* (1997), 6-7.

[60] US Department of Justice, *Report on the Availability of Bombmaking Information*, 5.

[61] Ken Shirriff, *The Anarchist Cookbook FAQ* (2001), <http://www.righto.com/anarchist-cookbook-faq.html> (12 Dec. 2005).

[62] Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet*, 9.

[63] William Powell, *The Anarchist Cookbook* (Ozark PR LLC, 2003 (1971)).

[64] Eugene Spafford, *Testimony before the US House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities*, 24 July 2003, 31, <http://commdocs.house.gov/committees/security/has205260.000/has205260_0f.htm> (12 Dec. 2005).

[65] Niall McKay, "Do Terrorists Troll the Net?" *Wired*, 4 November 1998, <www.wired.com/news/politics/0,1283,15812,00.html> (12 Dec. 2005).

[66] Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," 17.

[67] Richard Rogers, "Operating Issue Networks on the Web," *Science as Culture* 11, no. 2 (2002): 191.

[68] Soo Hoo, Goodman, and Greenberg, "Information Technology and the Terrorist Threat," 140.

[69] *Staff Statement No. 11, The Performance of the Intelligence Community* (Washington DC: 9/11 Commission, 2004), 9, <http://www.9-11commission.gov/staff_statements/staff_statement_11.pdf> (12 Dec. 2005).

[70] The project's Web site is online at <http://www.fas.org/sgp/>.

[71] John Lasker, "Watchdogs Sniff Out Terror Sites," *Wired News*, 25 February 2005, <http://www.wired.com/news/privacy/0,1848,66708,00.html> (12 Dec. 2005).

[72] John R. Bradley, "Website Postings Give Away Terror Activities," *The Straits Times*, 5 May 2004, <http://www.asiamedia.ucla.edu/article.asp?parentid=10916> (12 Dec. 2005).

[73] *Staff Statement No. 9. Law Enforcement, Counterterrorism, and Intelligence Collection in the United States prior to 9/11* (Washington DC: 9/11 Commission, 2004), 8, <http://www.9-11commission.gov/staff_statements/staff_statement_9.pdf> (12 Dec. 2005).

[74] Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw-Hill Osborne, 2003), 220.

[75] *Staff Statement No. 11, The Performance of the Intelligence Community*, 10.

[76] Bernhard Warner, "Experts Comb Web for Terror Clues," *The Washington Post*, 12 November 2003, <http://cryptome.org/web-panic.htm> (12 Dec. 2005); see also Associated Press, "Man Hijacks Al-Qaeda Site for FBI Use," *USA Today*, 30 July 2002, <http://www.usatoday.com/tech/news/2002-07-30-al-qaeda-online_x.htm> (12 Dec. 2005).

[77] Stephanie Gruner and Gautam Naik, "Extremist Sites under Heightened Scrutiny," *The Wall Street Journal Online*, 8 October 2001, <http://zdnet.com.com/2100-1106-530855.html?legacy=zdnn> (12 Dec. 2005); Richard Norton-Taylor, "MI5 Posts Terror Appeal on Arab Websites," *The Guardian*, 26 October 2001.

[78] Pew Internet and American Life Project, *One Year Later: September 11 and the Internet* (Washington DC: Pew Internet and American Life Project, 2002), 33-37, <http://www.pewinternet.org/pdfs/PIP_9-11_Report.pdf> (12 Dec. 2005).

[79] Lucy A. Dalglish, Gregg P. Leslie, and Phillip Taylor, eds., *Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know* (Arlington, VA: The Reporters Committee for Freedom of the Press, 2002), 25, <http://www.rcfp.org/news/documents/Homefront_Confidential.pdf> (12 Dec. 2005); Pew Internet and American Life Project, *One Year Later: September 11 and the Internet*, 8-9; see also John C. Baker, Beth E. Lachman, Dave Frelinger, Kevin O'Connell, Alex Hou, Michael S. Tseng, David T. Orletsky, and Charles Yost, *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information* (California: Rand, 2004), <http://www.rand.org/publications/MG/MG142/>.

[80] Dalglish, Leslie, and Taylor, *Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know*, 2; Guy Gugliotta, "Agencies Scrub Web Sites of Sensitive Chemical Data," *Washington Post*, 4 October 2001, A29, <//www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A2738-2001Oct3>(12 Dec. 2005); Pew Internet and American Life Project, *One Year Later: September 11 and the Internet*, 8-9; Julia Scheeres, "Suppression Stifles Some Sites," *Wired*, 25 October 2001, <http://www.wired.com/news/business/0,1367,47835,00.html>(12 Dec. 2005).

[81] Dorothy Denning, *Is Cyber Terror Next?* (New York: US Social Science Research Council, 2001), 1, <http://www.ssrc.org/sept11/essays/denning.htm> (12 Dec. 2005); National Infrastructure Protection Center, *NIPC Daily Report*, 18 October 2001.

[82] Charles Hauss and Alexandra Samuel, "What's the Internet Got to Do With It? Online Responses to 9/11" (paper presented at the American Political Science Association Annual (APSA) Annual Convention, Boston, 29 September-1 August 2002).

[83] Hauss and Samuel, "What's the Internet Got to Do with It? Online Responses to 9/11;" National Infrastructure Protection Center, *Cyber Protests Related to the War on Terrorism: The Current Threat* (Washington DC: National Infrastructure Protection Center, 2001), <http://www.iwar.org.uk/cip/resources/nipc/cyberprotestupdate.htm> (12 Dec. 2005).

[84] Institute for Security Technology Studies (ISTS), *Cyber Attacks during the War on Terrorism: A Predictive Analysis* (Dartmouth College: Institute for Security Technology Studies, 2001), <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm> (12 Dec. 2005).

[85] In Hebrew, 'Haganah' means defense. Internet Haganah is online at <www.haganah.org.il/haganah/index.html> (12 Dec. 2005).

[86] The SITE Web site is at <http://www.siteinstitute.org/> (12 Dec. 2005).

[87] Lasker, "Watchdogs Sniff Out Terror Sites."

[88] Lasker, "Watchdogs Sniff Out Terror Sites."

[89] Arquilla, Ronfeldt, and Zanini, "Networks, Netwar and Information-Age Terrorism," 66; Charles Piller, "Terrorists Taking Up Cyberspace," *Los Angeles Times*, 8 February 2001, A1.

MAURA CONWAY is a Lecturer in the School of Law & Government at Dublin City University and a PhD candidate in the Department of Political Science at Trinity College Dublin, Ireland. Her research interests are in the area of terrorism and the Internet. She is particularly interested in cyberterrorism and its portrayal in the media, and the functioning and effectiveness of terrorist Web sites. Along with a number of book chapters, Maura has also published in *First Monday*, *Current History*, the *Journal of Information Warfare*, and elsewhere. *Address for Correspondence*: Department of Law & Government, Dublin City University, Glasnevin, Dublin 9, Ireland; *E-mail*: maura.conway@dcu.ie.

BUILDING A SOUND AND FLEXIBLE EMERGENCY RESPONSE SYSTEM: HARD WON LESSONS IN DISASTER MANAGEMENT

George HANDY, John KIMBALL, and Jeffrey WINBOURNE

Abstract: Emergency management systems' failure to mitigate the devastation caused by hurricane Katrina imposed a number of unfortunate lessons from this disaster, lessons hard won and learned. These lessons are worth repeating for the benefit of the international emergency management community. Lessons this paper seeks to convey: the significance of organization and leadership, with communications as the critical link between them, to advance disaster responsiveness. Particular emphasis is placed on the role of communications, in its multiple modes, as it applies to disaster response management relevant to both Bulgaria and the Black Sea Basin/ Balkan region.

Keywords: Emergency Response System, Disaster Management, Hurricane Katrina, Leadership, Organization, Communications.

From our perspective, effective national response to disaster situations demands the following three core capabilities:

- *Organization*: Decentralized action and reaction bolstered by intense centralized operational support, organization, and policy direction, involving cooperation between civil and military government organizations, the private sector, and neighboring countries;
- *Leadership*: Leadership skill at all levels of the response to organization to motivate responders and direct cooperative action at all levels;
- *Communications*: Effective and timely sharing of information with emphasis on how, and how much information is acquired, how much and how frequently that information is shared, and how it is protected.

INFORMATION & SECURITY. An International Journal, Vol.19, 2006, 31-38.

Unifying Theme

Effective use of organization and leadership requires timely, accurate, and fully functional communications. Local response units must be able to communicate their situation, and paint an accurate picture of the incident to their commander and upward, or to operational support and senior leadership. Communications may range from "situation stable" status reports, to requests for a wide variety of assistance while indicating its urgency. The aftermath of hurricane Katrina suggests much needed scrutiny of the communication systems between federal, state, and local leadership.

Organization

Emergency management entities plan, prepare, and respond to a variety of crisis situations. Emergencies might range from manmade incidents, such as a chemical-biological threat to the New York City subway system, to that of a hurricane the size and force of Hurricane Katrina. Organization allows resources to anticipate and effectively manage disaster response, minimizing loss of life and property. Ability to implement pre-designed plans plays a key organizational role in effective emergency responsiveness. However, the ability to communicate with all assigned organizational units, and to deploy assigned resources in a timely manner, is critical to the successful organization of any emergency situation.

Example: A suspect agent is discovered, and appears to be chemical-biological in nature. First responders associated with local jurisdictions request more sophisticated testing and analysis of the suspect agent. What constitutes communications procedure? Several actions occur simultaneously: The on-site first responders take appropriate action based on local protocols and their knowledge of the situation. Requests for advanced analytical resources are simultaneously communicated up the chains of command. Needed resources are drawn from national, interagency, and/or private sector resources, and regional and international entities. The level of resources required dictates the entity appropriate to the task.

A natural disaster, such as a flood or an earthquake, exacts similar responsiveness. On-scene first responders recognize the need for advanced search and rescue capabilities, as well as extensive and immediate evacuation and transportation assets. The support for these tactical requests can be provided at all levels of national response. Neighboring jurisdictions may support evacuation and search and rescue at their level of capability. Assistance from neighboring countries and international search and rescue organizations may be requested concurrently at the appropriate national senior leadership level.

Hurricane Katrina impacted a geographic area approximately the size of Great Britain. Over 100 jurisdictions from local, state, and federal levels responded. Hundreds of non-government organizations also engaged, including the International Association of Fire Fighters and the National Organization for the Disabled, legitimate and valuable provisions of disaster response. Katrina's response requirements were obscured by the complex nature of lost assets, including fire protection, emergency medical services, and law enforcement. Entire infrastructure systems were obliterated, including those that provided food, water, housing and energy, as well as provisions for special needs populations. Countless industrial facilities in the region were almost completely destroyed. The national energy infrastructure was adversely impacted and numerous, major chemical spills migrated from the facilities, greatly adding to the local flood damage.

Without rapid and accurate communication systems, situations such as those described above become breeding grounds for rumor, panic, confusion, needless human suffering, excessive property loss, and probable loss of life. Such outcomes are preventable with the use of modern communication systems, comprehensive planning efforts, as well as aggressive training and exercise programs.

Leadership

Leadership guides and motivates responders to the extent that it has sufficient knowledge of the situation. Knowledge and preparation bolster responder confidence. The leader armed with critical and accurate on-site details performs based on pre-defined action plans, and instills response forces with confidence and unity. Such leadership provides motivational messages across geographic and political borders.

Mayor Giuliani's response following the September 11, 2001 terrorist attack in New York City illustrates this point. During the aftermath of the attack, the mayor gave direction to city resources responding to the attack, to the people of New York City, and to the nation. His ability to communicate with both general population and first responders was a critical element in providing leadership, rallying first responders to manage the tasks at hand, and addressing individual and societal feelings of grief and rage. As a leader, he understood his responsibility for managing local and national response to the attack. Several years prior to the attack, Mayor Giuliani advocated establishing the City's Office of Emergency Management. He recognized the role of organization, coupled with a sound communications infrastructure, as a critical tool for effectively managing emergency situations.

Another critical leadership concern involves effectively balancing competing demands for resources. The following illustrates the impact of pre-disaster planning at a national level: According to a US Government Accountability Office (GAO) report,

more than 75% of next year's Department of Homeland Security's preparedness grants convert to state and local readiness for anti-terrorism resources. The leadership of the National Emergency Management Association identified the problem. It warned DHS leadership that the change, including more proposed reductions of the Federal Emergency Management Agency (FEMA) role, weakened readiness for disaster response. Shifting resource allocation inappropriately to one DHS mission at the expense of another downplayed the role of emergency and disaster planning and response, and its overarching need to improve interoperable communications between emergency responders at all levels.

The conclusion and challenge: A disaster scenario requires leadership responsiveness to the dynamic, real-time demands of the situation. It must possess a foundation of solid preparation, effective organization, and comprehensive communications capabilities on which to rely. Additionally, prior to a disaster, leadership must provide strategic policy direction required for funding and support of preparedness measures.

Communications

Communications observably enables the bond between leadership and organization. When first responder units cannot communicate with the command structure or with each other, they became isolated and ineffective. If organization cannot communicate with both leadership and on-site units, effectiveness of units becomes marginalized.

Communication inadequacies between diverse units of first responders were patently critical to the Katrina response, especially with failure of existing electrical and telecommunications infrastructure. Planning for future events such as Katrina requires rethinking current approaches to communications technology. Use of independent communications platforms such as those used by the military becomes critical to future planning. Satellite communications, which received much attention after September 11, require consideration for use in all-hazards scenarios. The design and location of emergency communications centers and operational command centers also requires addressing. The new design must proceed from consequences: the over 50 centers that were inoperable for a time, or completely destroyed. Essential to disaster planning and communications is a high degree of reliability and redundancy for the response center buildings, their base-building systems, as well as the voice, data and video systems used by center personnel.

The impact on communications of both Katrina and September 11th emphasizes our dependence on existing infrastructures. The magnitude of Katrina's destruction prevented first responder units from communicating for reasons including equipment and frequency incompatibility, with all telephone system types effectively under water and out of service. September 11th first responders experienced similar, well docu-

mented, communications problems. The city's electrical grid was severely impacted, limiting power to radio and telephone systems that primarily, and in many cases, depended on it exclusively for powering these systems.

Another significant communications issue to consider involves discerning how much information should be passed through the chain of command's varying levels. Information overload becomes a common problem at emergency incidents of all types. Technology assists in classifying the type of information and its transmission. However, the information must be acquired, analyzed, and transmitted from the incident to each succeeding level in the response continuum. This concept derives from a combination of communications technical expertise, and the knowledge, experience, and training level of those analyzing the information. Procedures must also be developed in this regard that guide personnel, and can be practiced in exercises and planning events for all-hazards scenarios.

First responders must be able to filter out what is immediately important to develop objectives, and to identify the resources needed to accomplish those objectives. This activity is repeated at each step up the chain of command. The frequency of information transmission and updates can be managed by adopting the Incident Action Plan (IAP) method. The IAP clarifies task level actions, tactical goals, and strategic objectives at each level or organization on a time-phased approach based on the priorities of the incident. The IAP is a tested and proven method for focusing the information flow, and enabling response managers at all levels to make better informed decisions based on accurate information. Not only is the IAP a format designed to assist in the decision-making process, it is also an excellent method of communicating the decisions, and evaluating the effectiveness of the decisions. Responders at each level should be empowered by procedures and activated by accurate information in order to perform immediate critical actions, and integrate those actions into the longer-term Incident Action Plan. Responder and other personnel should not be burdened with information they do not need.

One of the immediate lessons learned from the effects of Hurricane Katrina concerns leadership, and its ability to capture and accurately interpret information. While much of the discussion surrounding real and perceived failures of governmental disaster response is skewed by natural human emotions, and fueled by the extent of the disaster and the personal hardships incurred, analytical conclusions can be drawn. Leadership at all levels lacked an accurate picture of the size, scope, potential, and extent of the storm and its resultant impact. While responders at all levels performed to the limits of human endurance and beyond, deficient information caused by poor or non-existent communications resulted in less-than-informed decisions and planning by leaders at every level.

Today's fast developing emergency situations, with increasingly capable communications technology, establishes information sharing systems as the cornerstone for emergency response. These systems are expected to rapidly and unerringly receive current disaster descriptions, assign resources, and modify standing policies and orders when appropriate. Additionally, leadership, through the emergency communications systems, is expected to quickly shift resources as the initial crises are mitigated, and more serious requirements identified.

Bulgaria's Emphasis on Information Sharing

Bulgarian planning for emergency management system modernization reflects each of these three capabilities, leadership, organization, and communication, with a priority on improving the latter. The present system limits efficient transmission of information between first responder agencies, including police, fire, and emergency medical. As we understand it, the Bulgarian Civil Protection Agency (CPA) is establishing an all-hazard response capability to address recurring natural hazards such as earthquakes and floods, as well as assigning appropriate emphasis to threats such as terrorism and hazardous waste. Additionally, CPA currently addresses technical infrastructure challenges, ranging from emergency communications capabilities to new communications requirements associated with integration into NATO and the European Union (EU). Establishing national communications architecture for civil protection information sharing, including interoperable systems supporting all-hazards operations, presents a clear challenge.

A recently published document of the US Department of Homeland Security Office of the Inspector General, "OIG-05036" detailed some critical conclusions concerning information technology applicable to Bulgaria and the Balkan/ Black Sea region. The report concerned assessing the strengths and weaknesses of the DHS Emergency Preparedness and Response Directorate to support incident response and recovery operations. The report highlights the DHS response to the previously unprecedented hurricane season of 2004 in which the east coast of the US was stuck by four hurricanes and one tropical storm in under three months. The report confirmed that the incident management system and the information technology needed to support such repeated responses was adequate to meet most of the challenges presented by these storms. However, the report indicates that the system was stressed nearly to the breaking point.

The conclusions and recommendations of this report were unfortunately validated by hurricanes Katrina and Rita in 2005. These include the following points:

- Modernization of outdated and dysfunctional legacy IT systems, including development and construction, which must support the national and regional

strategic goals and operational objectives of disaster planning and response. The IT strategic plan must reflect the national strategic plan, and IT systems must integrate to effectively support information exchange during response and recovery operations.

- Long-term solutions are far preferable to short-term fixes, especially when the existing infrastructure is outdated and based on similarly outdated organizational processes.
- Updating must include adequate requirements definitions, alternatives analyses, and sufficient tests prior to deployment

Reliable and Flexible Solutions

The manner in which the command, control and communications systems connect the first responder with city, province, and national leaders must improve logistical support, timely shifts in priorities, and deployment of first responder resources for an effective emergency response.

The following are considerations for how the solutions can be achieved:

- Leverage technology to insure agility and reliability in response to changing conditions, and planning for all-hazards conditions.
- Ensure effective decision-making through informed leadership and organization.
- Test leadership, systems, and organization through routine, “real-life” planning exercises.

Concluding Thoughts

By examining past emergencies and the current planning of major U.S. cities, states, and the national government, two measures of success stand out: establishing an effective single point of leadership for emergency response, and correctly managing first tasks in an emergency. Both leadership and first tasks depend upon effective information sharing through modern command, control, and communications systems. Determining the “first task,” or priory tasks, depends upon trained, experienced leaders familiar with the disaster scenario they are facing.

Without reliable, redundant, and competent communications to acquire and transmit useful information, even the finest leaders and response organizations face probable failure. Conversely, in the absence of trained leaders and organizations, the most robust communication system composed of state-of-the-art technology becomes a waste of national resources.

A national emergency management program requires leadership that provides strong strategic direction. Critical to strategy is its link to an organizational development plan of training, drills, and exercises. The national organization should be complemented by local and regional organizations that utilize the same operating protocols and procedures customized to local conditions. Linking this constellation of organizations and resources requires resilient, multi-mode communications systems that can withstand the results of a variety of natural and manmade disaster scenarios. Failure to integrate information technology systems with organization, planning, procedures, and training indicates failure of government in its duty to protect its citizens. Without this approach, the hard won lessons taught by both Katrina and September 11th will fail to have been fully learned, and the consequences doomed to become recurring themes at future disaster scenes.

GEORGE HANDY works for the Center for Strategic and International Studies (CSIS), concentrating for over 14 years on Eastern and Central European issues. He also serves as a Senior Advisor to Winbourne & Costas, Inc. regarding Eastern and Central European regional issues and emergency management.

JOHN KIMBALL is the Director of Emergency Management Services with Winbourne & Costas, Inc. He has over 20 years of emergency management experience working with the US Federal Emergency Management Agency (FEMA), and the US National Fire Academy. He has worked in many countries on emergency management issues, including: Bulgaria, United Arab Emirates, Macedonia, Greece, Turkey, Saudi Arabia, Singapore, and others.

JEFFREY WINBOURNE is the President and a founder of Winbourne & Costas., Inc. He is a recognized expert on emergency communications. He has provided expert advice to US cities including Washington, DC, New York City, Philadelphia, and Miami.

Winbourne & Costas, Inc. is a US-based firm that specializes in emergency management and communications consulting services.

RESEARCH AND DEVELOPMENT OF AN IRIS-BASED RECOGNITION SYSTEM FOR IDENTIFICATION AND SECURE AUTHENTICATION

Hussein H. FAKHRY and Benedict Bernard CARDOZO

Abstract: New developments in Iris recognition technology provide increased potential for security. The research study described in this article has been conducted to further explore its potential through the development and evaluation of a working prototype system for Iris Administration and Organization Resource Access Control. The developed prototype possesses Iris administration functionality with such functions as enrollment, identification, verification, update and deletion. Also, the prototype organization module allows management of organizational resources access control. Testing of the prototype has been performed at the Dubai Naturalization and Residency Department (DNRD) site. The test has demonstrated the usefulness of Iris authentication for automating passport control. Special Application Programming Interface (API) licensed from Iridian Technologies has been used in this development.

Keywords: Iris Recognition, Biometric, Security Access, Iris Authentication.

Introduction

Iris recognition is a biometric technology for identifying humans by capturing and analyzing the unique patterns of the iris in the human eye.[1] Iris recognition can be used in a wide range of applications in which a person's identity must be established or confirmed. For example, these include passport control, border control, frequent flyer service, premises entry, access to privileged information, computer login or any other transaction in which personal identification and authentication relies on knowledge-based or token-based passwords. Nevertheless, one of the most dangerous security threats in today's world is impersonation, in which somebody claims to be someone else. Through impersonation, a high-risk security area can be vulnerable. An unauthorized person may get access to confidential data or important documents can be stolen. Normally, impersonation is tackled by identification and secure authentica-

INFORMATION & SECURITY. An International Journal, Vol.19, 2006, 39-57.

tion, however, the traditional—knowledge-based (password) or possession-based (ID, Smart card)—methods are not sufficient since they can be easily hacked or compromised. Hence, there is an essential need for personal characteristics-based (biometric) identification due to the fact that it can provide the highest protection against impersonation. Among other biometric approaches, the new Iris recognition technology promises higher prospects of security.[2] Therefore, this research is conducted to further explore the potential of the Iris recognition technology and to demonstrate its potential through the development and evaluation of a working prototype.

Problem Definition

This research study explores the Iris recognition technology and develops a working prototype for an important application area – the Dubai Naturalization and Residency Department (DNRD), Dubai, United Arab Emirates. The application under consideration has a number of sensitive security issues, which could motivate the management of DNRD to implement the Iris recognition technology. A brief overview of DNRD and its basic activities is given in order to provide a better understanding of the issues.

History of Iris Recognition

The Iris recognition technology captures and analyzes the unique features of the iris in the human eye to perform identification. The algorithms recognizing persons by Iris recognition are very accurate to the extent that the entire planet can be enrolled in an Iris database with very little possibility of false acceptance or false rejection.[3] The first claim that no two irises are identical was made by Dr. Leonard Flom and Dr. Aran Safir, both ophthalmologists, in mid 1980s.[4] The claim was based on their clinical research that every iris is different and was seen to remain unchanged in clinical photographs. This claim made the human iris as a good candidate for a biometric solution and after substantial research the patent of using iris as a means for identifying persons was awarded to them in 1987.[5] Later in 1989, Dr. John Daugman developed algorithms for recognizing persons by iris recognition. The algorithms were patented in 1994 and nowadays they form the basis of all current iris recognition systems and products.[6]

Iris Characteristics

The human iris is a colored oval- to round-shaped ring surrounding the pupil of the eye. Figure 1 shows a sample iris.[7] It consists of muscles that adjust the size of the pupil. The iris is the only internal body organ that is visible externally. One of the most distinctive characteristics is its stability. The iris pattern stabilizes by the second

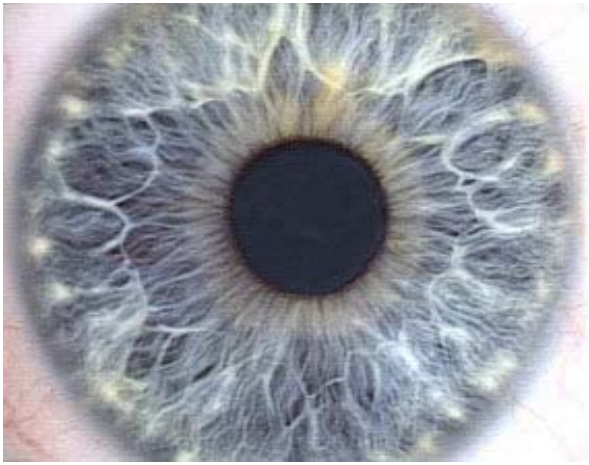

Figure 1: The Human Iris.[8]

year of birth and remains unchanged throughout person's lifetime unless injured or damaged by accident or disease.

The complex pattern of the iris contains many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette [9] that differentiate one iris from another. One of the major primary visible characteristic is the trabecular meshwork tissue, which gives the appearance of dividing the iris in a radial fashion.[10] This meshwork is formed permanently by the eighth month of gestation. Another important factor is that during development of iris there is no genetic influence on it, which is proved by a process known as "chaotic morphogenesis" occurring at seventh month of gestation. This means that even identical twins have completely different irises. As the iris is small in radius (about 11mm), it is a problem to get an image. However, it has great mathematical advantage because its pattern variability among different persons is very large.[11] This is due to the fact that the iris has more than 266 degrees of freedom,[12] which is the number of variables in the iris pattern that allow it to differ from another iris.

Other iris characteristics that make it appealing for authentication are:[13]

- The iris pattern is more complex and more random than other biometric patterns and hence offers a highly precise method for individual authentication with a false acceptance error rate of less than one in two million records.
- The iris located in the human eye is protected behind the eyelid, cornea and aqueous. This helps it to keep the damage and abrasion minimal. In addition, it is nearly impossible to forge identity.

- The iris pattern remains stable and unchanged after the age of two years and does not degrade over time or with the environment.
- The probability of two irises producing the same numerical code is almost zero.
- A distinctive iris pattern is not susceptible to theft, loss or compromise.
- Each iris is different, even between identical twins or between left and right iris of an individual.
- Since the iris is an extremely complex structure, modification of the iris would require sophisticated intricate microsurgery. This could result in individual loss of sight or an obvious artificiality that can be easily seen visually or through image analysis.

Physical Access Systems

This section describes some of the widely used commercial applications using the iris recognition technology for controlling and monitoring physical secure access to restricted areas and resources.

IrisAccess® 2200T System

Iridian Technologies and LG Electronics have teamed up together to create the IrisAccess® 2200T system.[14] The system is used to identify and authenticate user access to physical areas. The system designed and developed using Iridian Technologies' Iris recognition software and LG's imaging platforms delivers superb accuracy, speed, scalability and convenience for user identification and authentication. Some of the features of the IrisAccess® 2200T system are summarized below.

The imaging device automatically detects that a subject is approaching. The individual has to glance at the imaging device from a distance of 3–10 inches, which captures the iris image and digitally processes it to form a 512 byte IrisCode® template.

A patented search function enables real time database matching at remote unit level. User access is granted immediately as soon as the presented IrisCode® matches a valid IrisCode® template in the database.

Using organization Intranet and encrypted transaction, TCP/IP communication, the system can control the access to the secure area within the organization and up to 254 doors over the Internet.

Other features include audio interface in multiple languages, non-intrusive, one to many search identification and optional verification mode.

EyePass™ System

The EyePass™ System developed by EyeTicket Corporation [15] is primarily aimed at aviation industry. It is an access control service provided to air carriers, airport authorities and other large employers. Some of the features of the EyePass™ system are:

- Access control to secure areas for pilots, flight crews and ground staff at airports and corporate installations.
- Time and attendance functions are automated and secured by the system.

JetStream™ System

The JetStream™ System also developed by EyeTicket Corporation is used for positively identifying and authenticating passengers traveling on airlines. It is used in conjunction with the airlines' reservation system. Some of the features of the JetStream™ system [16] are: (1) Simplifies and expedites transactions providing maximum security and risk management at a competitive cost; (2) Allows passengers' to check in and board an aircraft simply by using one's iris. The JetStream™ system is a fully developed proven solution currently deployed at London Heathrow Airport.[17] Other application areas using the JetStream™ system include immigration control, railways and hotel industry.

Information Security

This section describes a commercially available application based on the iris recognition technology that addresses the issues of password management and uses one's iris as a positive identity to authenticate the access to data and information.

Panasonic Authenticam™

Iridian Technologies and Panasonic have teamed up to design and develop a system that primarily addresses issues related to passwords, PINs and token cards. Panasonic's Authenticam™ (see Figure 2) enabled with unique PrivateId™ software from Iridian Technologies allows the iris recognition camera to capture, select and secure iris images.[18] Some of the important features of the system are summarized below.

Panasonic's Authenticam™ enables system administrators to secure access to personal computers, files, folders, and applications only to authorized users. It uses the PrivateID™ software, which generates IrisCode® compatible with KnoWho™ Authentication Server from Iridian Technologies. Also, it includes the I/O software SecureSuite™, which allows multiple users to securely access restricted resources. The cost associated with password management and the risks of fraudulent activities are substantially reduced.

Figure 2: Panasonic's Authenticam™ Enabled with Private Id™ Software.

Authentication Server

The KnoWho™ Authentication Server from Iridian Technologies is designed to integrate with mission critical applications, transaction systems, network environments that require high performance authentication capabilities.[19] The authentication server is a major component used to store IrisCode® templates and to process the authentication. The Authentication server has two main functions, first to store IrisCode® templates and second – a processing engine that performs real-time matching. The KnoWho™ Software Development Kit (SDK) allows customization of the Authentication server capabilities for other applications. Some of the features of the KnoWho™ Authentication Server are [20]:

- Identification/ Recognition: one-to-many matching.
- Verification: one-to-one matching.
- Ability to enroll, update and delete new and existing IrisCode® templates, data etc.
- Use of Oracle 8i and SQL Server RDBMS to store IrisCode® and related data.
- Compatible with PrivateID™ supported cameras such as Panasonic Authenticam™.

- Data encryption at database level.
- Option to store facial images.

System Development Approach

Three approaches to system development have been considered and compared, namely the System Development Life Cycle (SDLC), the Object-Oriented Development (OOD), and the Rapid Application Development (RAD).

However, the RAD approach has been preferred for the following reasons:

- The main components and functions of the proposed system such as iris enrollment, recognition, verification and deletion are implemented using the pre-existing class libraries (API) licensed from Iridian Technologies. Hence, the RAD approach is suitable for fast development of the remaining components of the proposed system.
- Using RAD, the development of the system can be accelerated so as to prove and demonstrate to the management of DNRD as well as to other interested organizations the benefits of using a superior biometric technology to achieve a competitive advantage in solving their security problems.
- Through RAD, the project requires fewer resources and less time to rollout the final product resulting in reduced project costs.
- The final product is aimed at highly specialized information systems market and its distribution will be focused at in-house market for example at industries or at government establishments and quick development of the system can only make this possible.
- Using RAD helps in combating scope and requirements creep by limiting the project exposure to change – since changes are very much inevitable in long development processes such as in the System Development Life Cycle (SDLC) and the Object-Oriented Development (OOD) approaches, which can lead to significant expenses and waste of time and effort for redesigning and redevelopment.

Therefore, the RAD approach has been used to efficiently develop a reliable and robust prototype system while taking into consideration the continuous feedback from higher management executives, analysts and users.

Features of the Proposed System

The development of the proposed Iris Administration and Organization Resource Access Control System (illustrated in Figures 3 and 4) required development of four different modules which are:

1. Iris Administration.
2. Organization Resource Access Control Management.
3. Authentication and Secure Access to a protected resource using one's iris.
4. Link and Automate passport control for DNRD. It links the newly captured iris with DNRD's existing customer record in the database and automates Passport Control at Dubai International Airport.

The possible features of each module are summarized below.

1. *Iris Administration*

- Enrollment: The system should capture left, right and face images of a subject as well as his/her personal details and include/register the person in the biometric and application databases, respectively.
- Recognition: The system should retrieve all details of the person including iris and face images when one's iris is provided for identification.
- Verification: The system should verify the person by comparing the data and iris provided.
- Update: The system has to provide modification of personal data.
- Deletion: The system should permit, when needed, deletion of all personal data and the relevant biometric data from the application and biometric databases, respectively.

2. *Organization Resource Access Control Management*

The system allows adding and deleting resources from the organization hierarchy tree; however, in the presented research, the organizational resources are pre-defined.

The system retrieves the details of the enrolled person based on some criteria such as name, personal identification number, etc. Using the retrieved data, the system grants access to a resource for a single or many persons. Using the retrieved data, the system might also revoke access to a resource for a single or many persons. The system displays the granted resources for a person.

3. *Authentication and Secure Access*

The system should be able to grant access to a protected resource. The protected resource simulated for this particular project is the information data main menu that is given access to by using one's iris or optionally by entering user login name and password. The organizational resources access control module manages the access to the main menu options. In case of a failure of the biometric system, the system should permit to the user access to the protected resource by using his/her login name and

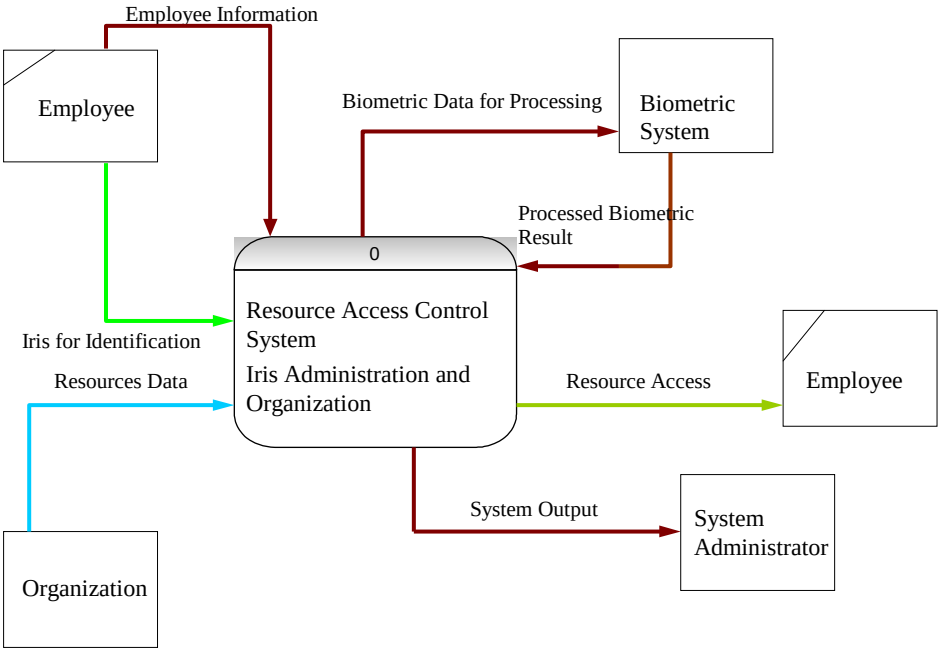

Figure 3: Context Diagram of the Proposed System.

password. Only the menu options that are granted access to should be enabled, whereas others should be disabled.

4. *Link and Automate Passport Control for DNRD*

The system will use the existing program module from DNRD to link its customer database with the enrolled person. The customer could expedite his/her passport and immigration checks by providing his iris – the system will automatically make an entry or output record for the person in the DNRD database.

Development Environment

The development environment consists of the technologies, programming languages, standards, protocols and tools that are used in developing the Iris Administration and Organization Resource Access Control System. The major components used for building the prototype system described in this article are the PrivateID™ and KnoWho™ Authentication Server APIs from Iridian Technologies. The other components in the development environment are ActiveX control developed using Microsoft Visual C++, Form Builder v6 in Oracle Developer 2000 environment and

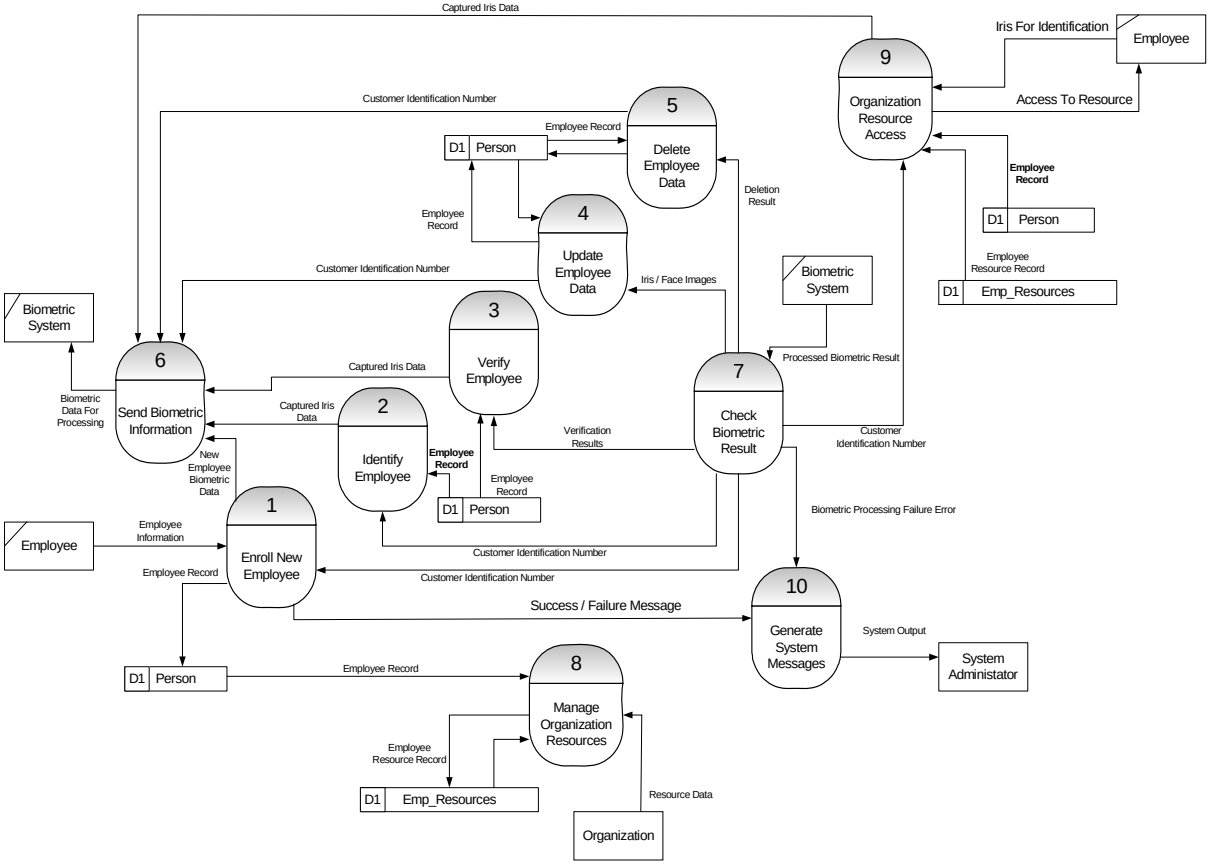

Figure 4: Level 0 Data Flow Diagram of the Proposed System.

Oracle 8i Relational Database Management System (RDBMS). Figure 5 illustrates the system components, highlighting the components developed in this study.

PrivateID™ and KnoWho™ Authentication Server

PrivateID™ and KnoWho™ Authentication Server can be integrated into new or existing systems. The open architecture of both PrivateID™ and KnoWho™ Authentication Server makes it possible to integrate the iris recognition technology into distributed applications such as Internet applications.

It also makes the network security solutions easy to implement.

The basic components include:

1. PrivateID™ software – image capturing software that runs on clients' computers.
2. PrivateID™ enabled video camera such as Panasonic Authenticam™ with specialized lens for photographing the iris.
3. KnoWho™ Authentication Server – a highly secure and scalable transaction server.
4. Biometric Database – a RDBMS such as Oracle or SQL Server maintained exclusively by the KnoWho™ Authentication server.

A typical client-server application using PrivateID™ and KnoWho™ Authentication Server performs the following steps:

- The application running on the client side requests the PrivateID™-enabled video camera such as Panasonic Authenticam™ to capture an iris image of the subject.
- The PrivateID™ software would return the captured iris data to the calling application code.
- The application running on the client side would send the data to the server side of the application that calls the KnoWho™ Authentication Server API to perform biometric processing (e.g. perform recognition).
- The KnoWho™ Authentication Server would return a result to the calling application.
- Based on the result, the application would decide whether to grant or reject access to the protected resource.

PrivateID™ software

The PrivateID™ software allows an iris recognition enabled camera such as the Panasonic Authenticam™ to capture, select and secure iris images. The software was

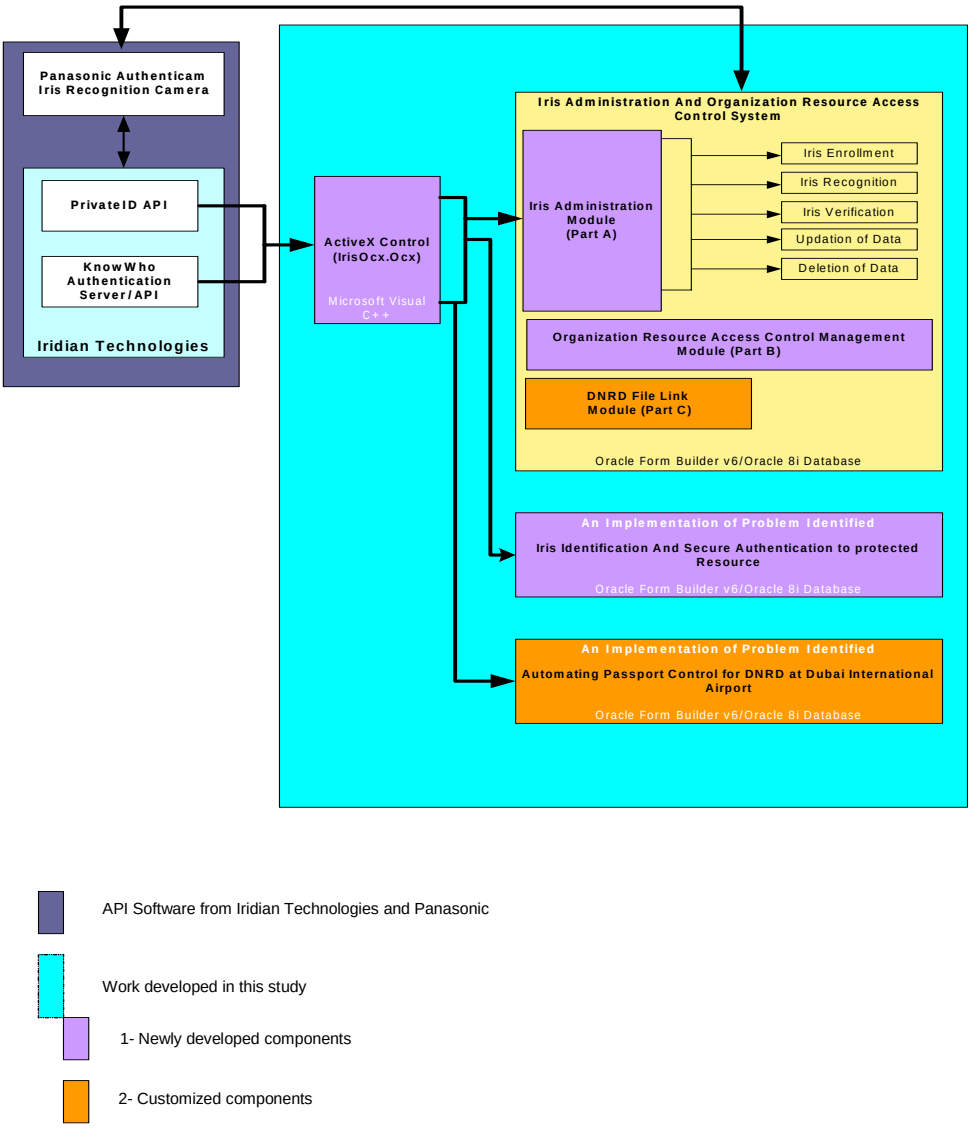

Figure 5: Components of the Developed System.

basically designed for information management and security. The only important function is capturing and selecting iris images for transfer and further processing for authentication.[21] The software captures a series of video digital images of the individuals' eye. The iris image is inspected for sufficient quality and content using

built-in image quality metrics within the software.[22] This ensures that the image provided to the server will have high confidence levels for a successful match outcome. The software also provides an audible beep just like the "closing of camera shutter" to inform the user that the image capture session is complete. A configurable timeout parameter can also be set for iris image capture session during which time if an image of high quality is not obtained, the whole process has to be repeated again. The image provided by PrivateID™ is in a compressed format. PrivateID™ and KnoWho™ Authentication Server work in single-factor authentication mode, requiring no other information in association with the record.[23] A nonce is used by the PrivateID software to prevent replay of transactions by a hacker or a third party software tool. A nonce is defined as an item that is used once and discarded.[24]

A nonce is a randomly generated number of 16 bytes that is concatenated to the iris image before it is encoded using either Blowfish or 3DES encryption methodologies. For the implementation of this project, 3DES encryption has been used. The encoded iris image with message authentication code (MAC) is sent to the authentication server. The authentication server uses its active 3DES private key to decode the iris image with MAC to continue with further processing.

Using such a technique, the Iris image becomes used one and discarded data package. Replay cannot be performed because the original nonce does not match any of the active nonces on the server either because it has expired, timed out or is not valid due to used-only-once policy.

PrivateID™ Application Programming Interface v2.1

The PrivateID™ Application Programming Interface (API) provides functions or interfaces that enable video capturing of the iris or the face.[25]

The CLCaptureIrisNonce function captures an iris image of suitable quality that will be sent to the KnoWho™ Authentication Server for biometric processing. This function is used with the nonce described in the previous section.

KnoWho™ Authentication Server

The KnoWho™ Authentication Server accepts the iris image sent via PrivateID™-enabled iris recognition camera, checks for image integrity and then performs the biometric processing requested by the client application, for example verification (1:1 matching) or identification (1:many matching). After validating the integrity of incoming data, it then creates an IrisCode template for matching the IrisCode templates that already exist in the system.[26] The KnoWho™ Authentication Server supports five main operations that include enrollment, verification, recognition, update and dele-

tion. The KnoWho™ Authentication Server stores three types of biometric information, which are as follows:

- IrisCode templates (left or right eye or both) stored in cache and on disk.
- Iris images (left or right eye or both) on disk.
- Portrait facial images (JPEG format, about 20 KB) on disk. The KnoWho™ Authentication Server stores only the individual identification number indexed with the IrisCode template. No personal data is stored, thereby ensuring privacy. Figure 4 depicts the individual privacy at KnoWho™ Authentication Server.

Passport Control Automation for DNRD

To automate the passport control process, two programs from DNRD were customized so as to link to the Iris Administration and Organization Resource Access Control System. In an all person inquiry program from DNRD, the employee data was retrieved from the DNRD database and a link was made with the enrolled employee data in the application database. Since the DNRD information is strictly confidential and sensitive, only the DNRD employee's file number was stored in the application database. The other program for passport control embeds the reusable ActiveX control component developed in this project. When the registered employee presents his/her iris, the CIN retrieved from the biometric database links with the PIN from the application database which in turn is linked to DNRD employee's file number. The employee's file number is used to retrieve the details from DNRD and automate the entry – exit transaction. Figure 6 displays the actual development of the system made in the course of this research study.

Testing Plan for the Developed System

Testing of the developed system is performed in two phases: unit testing and integration testing.

Unit Testing

In this phase, the ActiveX control component was tested for the following conditions using the ActiveX control test container available in Microsoft Visual Studio:

- Connectivity to KnoWho™ Authentication Server. To perform iris administration tasks, the ActiveX control component must be able to connect to the authentication server. The ActiveX component method 'GetServerStatus' is invoked to check the connectivity to the server.

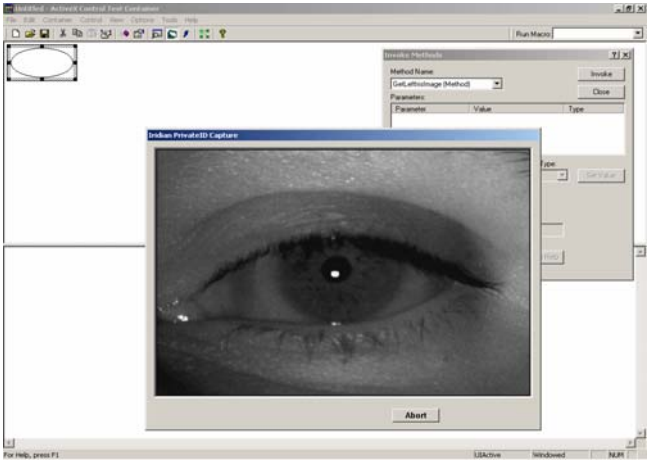

Figure 6: ActiveX Control Unit Testing for Left Iris Capture.

- Capturing of iris images. Another very important functionality of the ActiveX control is to capture iris images for the purpose of enrollment, identification and verification. Two methods are available for this purpose: GetLeftIrisImage and GetRightIrisImage. Figure 6 shows the PrivateID™ iris capture window when the method GetLeftIrisImage is invoked. The function returns zero if the capturing of the iris image is successful.

All remaining functions or methods of the ActiveX components were tested prior to integrating them with the application.

Integration Testing

Integration testing involves building the whole system using the final set of completely-tested individual program components and testing the resultant system for problems that may arise from interactions between the components.[27] To minimize errors and to find the source of error quickly, the incremental approach of adding and testing components is usually followed. The benefits of the incremental integration approach are:

- Errors can be found easily when the number of integrated components is small. This helps in locating and resolving the source of error quickly.
- A new component will be added only if the system with the existing components is completely error-free. In case of a new error, it can be easily attributed to the last added component.

The disadvantage of integration testing is that testing a system feature may require more than one component at a time to be integrated. Testing may find errors between individual components and other parts of the system.[28] Due to this fact, fixing errors can be difficult since it may affect the system functionality as all the components may change. Furthermore, introducing a new component may result in interaction error with previously integrated tested component.

Figure 7 illustrates how a staff member of the Information Technology section at DNRD tests the Iris administration and Organization Resource Access Control System.

Figure 7: DNRD Staff Testing the System.

Concluding Remarks

The research presented in this article has demonstrated the design, development and implementation of an efficient and reliable prototype using the iris recognition technology that has the potential to bring intangible benefits to organizations wishing to enhance or integrate new security policies for their protected resources. The iris recognition technology is the most accurate, fast and less invasive one compared to other biometric techniques using for example fingerprints, face, retina, hand geometry, voice or signature patterns. The system developed in this study has the potential to play a key role in areas of high-risk security and can enable organizations with means allowing only to the authorized personnel a fast and secure way to gain access to such areas. In particular, the developed system allows:

- Enrolling a person in the biometric system by capturing his/her irises.
- Accurately identifying (1:many search) a person by just capturing any of his/her irises.
- Verifying (1:1 search) a person by matching his/her data linked in the system with one's iris.
- Access for the enrolled employee to organization's protected resource by capturing his/her iris.

The Rapid Application Development approach used for design and development has delivered a highly robust and generic product, which can be easily customized for any other organization or industry. Moreover, the reusable ActiveX control component created for this system can be easily deployed in many Windows-based development tools. The presented system has been implemented using Panasonic's Authenticam™ with the Private ID™ software and the KnoWho™ Authentication Server from Iridian Technologies. To date, these are the only Application Programming Interfaces (API) available on the market. Almost all applications worldwide based on the iris recognition technology have these APIs integrated with them. Iris recognition can be used for physical access security, information data security, border control, automated passport control, banking, services and manufacturing industries. The list with potential application areas is open since iris recognition can serve many other purposes.

Notes:

[1] John G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence* 15, no. 11 (November 1993): 1148-1161.

[2] John G. Daugman, "Biometric Personal Identification System Based on Iris Analysis," U.S. Patent No. 5,291,560 issued March 1, 1994.

[3] John G. Daugman, "The Importance of Being Random: Statistical Principles of Iris Recognition," *Pattern Recognition* 36, no. 2 (2003): 279-291.

[4] Daugman, "The Importance of Being Random: Statistical Principles of Iris Recognition."

[5] Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence."

[6] Daugman, "Biometric Personal Identification System Based on Iris Analysis."

[7] John G. Daugman, "Sample Iris Image," <http://www.cl.cam.ac.uk/users/igd1000/sampleiris.jpg> (15 May 2003).

[8] Daugman, "Sample Iris Image."

[9] John G. Daugman, "Anatomy, Physiology, and Development of the Iris," <http://www.cl.cam.ac.uk/users/jgd1000/anatomy.html> (12 April 2006).

[10] Daugman, "Anatomy, Physiology, and Development of the Iris."

[11] Daugman, "Anatomy, Physiology, and Development of the Iris."

[12] International Biometric Group, "Iris-Scan: How It Works," <www.biometricgroup.com/reports/public/reports/iris-scan_tech.html> (12 April 2006).

[13] Daugman, "Anatomy, Physiology, and Development of the Iris."

[14] Iridian Technologies, "Iridian Technologies: Products," <http://www.iriscan.com/products.php> (14 April 2006).

[15] EyeTicket Corporation, "EyePass," <http://www.eyeticket.com> (5 May 2006).

[16] EyeTicket Corporation, "EyePass."

[17] EyeTicket Corporation, "EyePass."

[18] Iridian Technologies, "Iridian Technologies: Products."

[19] Iridian Technologies, "Iridian Technologies: Products."

[20] Iridian Technologies, "Iridian Technologies: Products."

[21] Iridian Technologies, "PrivateID and KnoWho Authentication Server Product Description," <http://www.iriscan.com/products.php> (15 April 2006).

[22] Iridian Technologies, "PrivateID and KnoWho Authentication Server Product Description."

[23] Iridian Technologies, "PrivateID and KnoWho Authentication Server Product Description."

[24] Iridian Technologies, "PrivateID and KnoWho Authentication Server Product Description."

[25] Iridian Technologies, "PrivateID for Windows API," January 26, 2002.

[26] Ian Sommerville, *Software Engineering*, 6th edition (Reading, MA: Addison-Wesley, 2001).

[27] Sommerville, *Software Engineering*.

[28] Douglas Bell, *Software Engineering: A Programming Approach*, 3rd edition (Addison-Wesley, 2000).

HUSSEIN FAKHRY, PhD, PEng is an Assistant Professor at Dubai University College, U.A.E. He received a PhD degree in Computer Control Systems and Robotics from University of Waterloo, Canada. Dr. Fakhry's research interests are mainly related to information systems, software engineering, computer control systems, robotics and applications of artificial intelligence. His current research interests include software systems architectures, modeling and simulation, IRIS recognition, and information systems security. He has worked for industry on many projects in control systems and SCADA systems. He is a member of a number of professional associations and networks including IEEE and IASTED.

BERNARD B. CARDOZO is a Senior Systems and Database Administrator at Dubai Naturalization and Residency Department (DNRD). He holds a Masters Degree (MSc.) in Computing and Information Systems from University of Hull, UK. Mr. Cardozo has more than 13 years of experience in the IT Industry. He has experience in the areas of project management, system analysis and design, programming, systems integration, database administration, distributed database architectures and data replication. He has been involved and has worked on major projects in DNRD such as Electronic Gate (EGATE) at Dubai Airport, Iris Recognition, Ports System and other major application modules.

The Terrorist Threat and the Response of the Armed Forces

- Does NATO Have a Role in the Fight against International Terrorism: Analysis of NATO's Response to September 11
- Special Operations Forces in the Fight against Terrorism on National Territory
- Terrorism on the Sea, Piracy, and Maritime Security

DOES NATO HAVE A ROLE IN THE FIGHT AGAINST INTERNATIONAL TERRORISM: ANALYSIS OF NATO'S RESPONSE TO SEPTEMBER 11

Krassimir KUZMANOV [1]

Abstract: This article analyzes NATO's decisions and actions taken in response to the 11 September 2001 terrorist attacks against the United States and assesses the probable future role of the Alliance in combating international terrorism. In September-October 2001, the United States chose to lead a coalition against the Al Qaeda terrorists and their supporters in Afghanistan instead of ceding the initiative to NATO. The necessity for rapid decisions and actions, the military capabilities gap between the United States and the European allies, and the lessons from NATO's air campaign in the 1999 Kosovo crisis, probably led the United States to make this choice. NATO's contributions to the campaign against terrorism have included sending Airborne Warning and Control Systems aircraft to the United States, deploying naval forces to the Eastern Mediterranean, and conducting preventive action against terrorist groups acting within or from the Balkans. Other measures taken by the Alliance include: adoption of a new Military Concept for Defence against Terrorism and a Partnership Action Plan on Terrorism, strengthening the nuclear, biological and chemical defence and civil protection, better cooperation with other international organizations, etc. NATO's responses to the 11 September attacks, the unconventional and asymmetric threat posed by international terrorism, and the distinct contributions that the military can make in combating terrorism support the main hypothesis of this article: that NATO may be unable to play more than specific limited roles in the fight against international terrorism.

Keywords: Counterterrorism, Active Endeavour, defence against terrorism, DAT, NATO response force.

Overview

The 11 September 2001 terrorist attacks were not the first conducted by foreign terrorists against targets on U.S. soil. The differences, however, between the 2001 attacks and the World Trade Centre bombing in 1993 include the results: the enormity

of the death toll, owing in particular to the demolition of the Twin Towers. The scale of the 11 September attacks revealed the vulnerability of the United States and its allies. Nevertheless, the 1993 bombing and the bombing of the Alfred P. Murrah Federal Building in Oklahoma City in 1995 had already proved that the United States could not remain safe from terrorism at home.

The West European states have had much greater experience in countering domestic terrorism; they have also encountered several terrorist attacks with international dimensions. Examples of such attacks include the Munich Olympics massacre in 1972 (9 hostages killed), the hijacking of the Lufthansa flight to Mogadishu in 1977 (all hostages rescued), the attacks on the Rome and Vienna airports in 1985 (19 people killed), the *Achille Lauro* hijacking in 1985 (1 passenger killed), the bombing of Pan Am Flight 103 over Lockerbie in 1988 (270 people killed), and the bombing of the French UTA flight over Chad in 1989 (171 passengers killed).

The world changed on 11 September 2001. This phrase, which has already become a cliché, applies to many areas of public life. Without any doubt, this date will leave a profound imprint on the history of the modern world. It has initiated processes that likely mark the beginning of a new epoch in international relations and global security. One of them is the first invocation of NATO's Article 5 in the history of the Alliance.

U.S. Decisions in Response to 11 September 2001

Defining the Enemy

A few hours after the attacks against the World Trade Centre and the Pentagon, the Federal Bureau of Investigation (FBI) revealed the identity of the hijackers: fifteen Saudis, two citizens of the United Arab Emirates, one Lebanese, and one Egyptian. The delayed travel bag of Mohamed Atta, the suicide pilot of American Airlines Flight 11 and presumed mastermind of the nineteen terrorists, provided a great source of information about the motives and the mindsets of the attackers.

Immediately after the attacks, suspicions about a possible link between Osama bin Laden and the attacks arose among U.S. officials. The former SACEUR, retired General Wesley Clark, suspected that bin Laden was responsible for the terrorist acts. Al Qaeda was considered the only terrorist organization capable of organizing and conducting such an operation. The "largest operation in the history of the FBI" soon gave results. Coordinated investigations in the United States and Germany discovered links between the attackers and Al Qaeda operatives in Germany. The results of the investigation gave President George W. Bush reason to declare before the Congress on 20 September 2001: "Our war on terror begins with al-Qaeda, but it does not end

there. It will not end until every terrorist group of global reach has been found, stopped, and defeated." [2]

The location of bin Laden was relatively clear: since 1996 he had enjoyed a safe haven in Afghanistan provided by the Taliban regime. The U.S. administration asked the Afghanistan government to surrender its "guest" to the United States. When it became obvious that the Taliban did not intend to cooperate, the United States started preparations for a retaliatory campaign. The short-term aims of the operation were that Osama bin Laden and the other perpetrators of the 11 September attacks be apprehended and brought to justice, that the Al Qaeda installations in Afghanistan be destroyed, and that the Taliban regime be toppled. The long-term objective was proclaimed by President Bush: a global war on terrorism (GWOT).[3] The four principles, on which the U.S. policy in this campaign has been based, were published in the State Department's *Patterns of Global Terrorism 2001-2003*. These principles include:

- Making no concessions to terrorists and striking no deals;
- Bringing terrorists to justice for their crimes;
- Isolating and applying pressure on states sponsoring terrorism to force them to change their behaviour;
- Bolstering the counterterrorist capabilities of those countries that work with the United States and require assistance.[4]

Defining the Mission and the Coalition

The short-term mission required a specific approach in defining the most appropriate coalition. The U.S. administration had to choose between at least three options in regard to the forthcoming campaign:

- The U.S. forces could act alone;
- The United States could organize a broad coalition; or
- NATO could take the lead and conduct the campaign.

The first option had probably been excluded in the very first days after 11 September. The disclosures about the international character of the terrorist network that conducted the attacks and the experience of other countries from their military campaigns in Afghanistan may have influenced the U.S. decision to seek broad international support for a U.S.-led campaign.

Afghanistan had historically been a graveyard for foreign invaders. Both the British and the Soviets had had bitter experiences in their campaigns in that country. A new foreign invasion could be used by the Taliban regime and the religious leaders to motivate large segments of the population to resist the invaders. Such resistance could

significantly complicate the tasks of the U.S.-led forces while giving additional time to the key Al Qaida leaders to evacuate.

These facts, the operational need for bases close to Afghanistan, and the risk that some terrorists might flee to neighbouring countries defined the need for coalition partners not only among Afghanistan's neighbours but also on a broader basis. The United States recognized that it could gain an important internal ally – the Northern Alliance, an armed group resisting the Taliban regime. The Northern Alliance was able to provide forces for the land offensive and could frustrate the Taliban's efforts to unify the population and organize national resistance against the foreign forces.

The U.S. decision to favour a U.S.-led coalition instead of a NATO-led coalition is one of the central themes of this article. The U.S. administration decided that the mission had to determine the most suitable coalition. The decision about the mission and the coalition was taken within a week after September 11. On 20 September 2001, Richard Armitage, the Deputy Secretary of State, informed the North Atlantic Council (NAC) of President Bush's efforts to arrange a grand coalition, which meant that the United States had decided to take the lead in organizing the impending campaign.

At least three considerations may have played a role in the U.S. decision to organize a U.S.-led broad antiterrorist campaign instead of a NATO-led operation: (1) the need to involve in the coalition a broad range of partners from all over the world – both states and sub-state actors (such as the Northern Alliance); (2) the preference to avoid constraints on U.S. latitude that might arise in a NATO-led operation and to guarantee the speed and freedom of an independent action through a U.S.-led campaign, i.e., to implement the lessons learned from the NATO-led Operation Allied Force in Kosovo; and (3) the capabilities gap between the United States and the other NATO allies.

International terrorism cannot be defeated by the unilateral efforts of a single country. In the words of the former U.S. Secretary of State, Colin Powell,

> In this global campaign against terrorism, no country has the luxury of remaining on the sidelines. There are no sidelines. Terrorists respect no limits, geographic or moral. The frontlines are everywhere and the stakes are high. Terrorism not only kills people. It also threatens democratic institutions, undermines economies, and destabilizes regions.[5]

An efficient fight against international terrorist organizations requires common and coordinated contribution in a wide range of areas: legislative, judicial, law-enforcement, military, financial, religious, etc. This option could provide the United States an opportunity to select which of the offered assets to accept and to request support in specific areas of the campaign against terrorism. Another important aspect in regard to the coalition participants was the United States to gain support and partners among

the Muslim states. This would prevent possible misinterpretations and speculations that might present the campaign against terrorism as a conflict between Christianity and Islam or as a war of Western civilization against Islamic civilization.

NATO's Cohesion versus Independent Action: Implications from Operation Allied Force

The strikes against Al Qaida and the Taliban military installations had to be fast, surprising, and effective in order to prevent Taliban forces from re-grouping and to prevent terrorists from escaping. Some of the targets (e.g., the top Al Qaida leaders) were dynamic and their capture was expected to be heavily dependent on intelligence support. Swift changes in the required strategy and tactics could also be expected. All these factors would demand rapid decisions. On the one hand, a NATO-led operation might increase the cohesion of the Alliance and provide NATO with new roles and missions for the 21st century. Additionally, NATO could increase its importance as a factor for international security, especially after conducting a successful operation far beyond its traditional area of responsibility. On the other hand, the United States had the experience and the lessons learned from its participation in Operation Allied Force in the Kosovo conflict in 1999.

The forthcoming campaign in Afghanistan "was not the kind of war that required large numbers of military personnel, and the command and control problems of a multilingual force away from familiar NATO terrain would have been challenging." [6]

> Only the British had the sealift and in-flight refuelling capabilities to get troops to the region under their own steam and to keep them supplied once in place… Allies might also have proved restrictive on American freedom of action, as NATO allies had an occasion been over target selection during the Kosovo bombing campaign.[7]

During the preparation and execution of Operation Allied Force, the United States faced several difficulties with the European allies. Some of these allies had internal policies or military capability constraints affecting their participation in the operation.

> Several Alliance members lacked domestic support for an offensive operation in Kosovo. In Greece, domestic opposition ran as high as 90 percent, and the Italian government feared that internal divisions over the operation could shatter its ruling coalition.[8]

The target approval process was another area in which different national policies and bureaucratic procedures affected the speed and the effectiveness of the operation and even the safety of the allies' aircraft. For instance,

> [w]hen Operation Allied Force commenced, NATO's Master Target File included 169 targets, of which 51 were initially approved. By the end of the operation in June 1999, it had grown to include more than 976 targets, enough to fill six volumes. Because NATO had not anticipated a long campaign, the newly nominated targets had not been developed fully in advance. Each of the additional 807 targets

> had to be proposed, reviewed, and approved by NATO and national authorities before being added to the master list. This cumbersome process revealed major divisions among the NATO allies and limited the military effectiveness of the operation.[9]

In addition, "parallel U.S. and NATO command and control structures and systems complicated operational planning and maintenance of unity of command." [10]

The United States also had concerns about sharing secret information with its NATO allies:

> Even when the United States decided to share information with its allies, the process of clearing and distributing that information did not flow smoothly. Delays and restrictions consistently hindered this process, which made it hard for the NATO allies to have a full operational picture.[11]

The Military Capabilities Gap: Implications from Operation Allied Force

The gap between the military capabilities of the United States and those of its European allies, which became obvious during Operation Allied Force, provoked concerns and debates in the Alliance. In his remarks at the Defence Week Conference, held in Brussels in 2000, Lord George Robertson, then NATO Secretary General, stated:

> The Kosovo air campaign demonstrated just how dependent the European Allies had become on U.S. military capabilities. From precision-guided weapons and all-weather aircraft to ground troops that can get to the crisis quickly and then stay there with adequate logistical support, the European Allies did not have enough of the right stuff.
>
> On paper, Europe has 2 million men and women under arms – more than the United States. But despite those 2 million soldiers, it was a struggle to come up with 40,000 troops to deploy as peacekeepers in the Balkans. Something is wrong and Europe knows it.[12]

Operation Allied Force demonstrated the imbalance between the U.S. and the European capabilities. The share of the U.S. contribution to the operation is impressive:

- 60% of all sorties;
- 80% of all weapons delivered;
- 95% of cruise missiles launched;
- 650 of 927 participating aircraft;
- 70% of all supporting missions;
- 320 B-52, B-1, and B-2 sorties dropped half of the total of bombs delivered;
- 90% of all EW (electronic warfare) assets;
- All stealth assets;
- All Airborne Command and Control facilities;

- Most of the equipment and manpower for the Combined Air Operations Centre in Vicenza;
- Most of the Air-to-Air Refuelling capability;
- 90% of the employed and vital mobile target acquisition capability;
- Most of the Air-to-Air Refuelling capability.[13]

According to David Yost, "European contributions in Operation Allied Force were particularly strong in combat air patrol; air-to-ground strike operations in good weather; and in surveillance, reconnaissance, and battle-damage assessment with unmanned aerial vehicles (UAVs) and manned aircraft." [14] However, "an average of three American support aircraft was required for each European strike sortie." [15]

These facts suggest that in a possible Alliance military operation far beyond Europe the burden for providing support to the allies would be much greater for the United States and could degrade the speed and the effectiveness of the operation.

Coalition Dynamics and Operation Enduring Freedom

The U.S. imperative in regard to the campaign in Afghanistan had been, in the words of the Defence Committee of the British House of Commons, "to strike quickly and with force against terrorists in Afghanistan and… the reality of the situation was that it would have been difficult to get all 19 NATO countries to act within the four week period which the US was able to achieve." [16]

The military phase of the campaign in Afghanistan, Operation Enduring Freedom, began on 7 October 2001 with cruise missile and air strikes on Taliban military installations and Al Qaida training camps. Great Britain was the only NATO ally that took part in the missile attacks and the air strikes at the beginning of the campaign. Another U.S. ally on the ground was the Northern Alliance. With U.S. air support and the assistance of small numbers of U.S. special forces, by 9 November 2001 the Northern Alliance captured the key city of Mazar-e-Sharif in Northern Afghanistan. On 14 November, the Northern Alliance entered the capital, Kabul. "Only after more than a month of fighting did the White House accept the allies' offers of thousands of combat and support troops, and then only in limited numbers and outside NATO's chain of command." [17] In this regard, Tomas Valasek wrote:

> Perhaps the most surprising aspect of the current counterterrorist operations is that the world's strongest military alliance, NATO, is nowhere in sight. The formerly 16, now 19, allies spent decades planning for jointly defending one another from an attack. Yet when the military operations began, the White House essentially asked NATO to stay out of the conflict, despite its offers of help and the gallant gesture of evoking the mutual defence clause in its founding document, the 1949 Washington Treaty, for the first time ever.[18]

NATO's Practical Support to the Campaign against Terrorism

The Article 5 Invocation

Immediately after the terrorist attacks, in the evening of 11 September 2001, the North Atlantic Council (NAC) declared that "the United States can rely on its 18 Allies in North America and Europe for assistance and support." [19] At that critical moment neither the U.S. government nor the NAC had reliable information about the origin of the attacks. The motives and the perpetrators were unclear; there was no claimed responsibility; and nobody set demands or conditions. The obvious facts were that three of the hijacked planes had completely demolished the Twin Towers of the World Trade Centre in New York and the west wing of the Pentagon in Washington, and had thereby caused thousands of deaths. The terrorist attacks were surprising and shocking; their enormity and barbarism were sobering for all; and the success of the attacks against the strongest NATO member revealed the vulnerability of each state and its institutions.

However, some of the European allies have had a greater experience than the United States has had in tackling domestic terrorism, and they knew that no one is assured against terrorist attacks. The perception of vulnerability, the solidarity with the United States, and the anger and indignation at the brutal terrorist acts unified NATO allies and their partners in their resolve to support the United States in the response to the challenge of terrorism. The lack of information about the terrorists and their motives and identity led to the conditional invocation of Article 5 of the Washington Treaty. The allies had to wait for the results from the investigation, which was to reveal whether the attacks were directed from abroad. This was set as a condition for the effective invocation of Article 5.

Article 5 defines the conditions upon which the principle of collective defence could be applied:

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.
>
> Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.[20]

The applicability of Article 5 to terrorist attacks against the United States requires additional analysis. Article 5, referring to Article 51 of the Charter of the United Nations, foresees the right of individual or collective self-defence in case of an armed attack against one or more allies. The condition for effective application of Article 5 in response to the 11 September attacks was a confirmation to be presented to the NAC that the attacks were directed from outside the United States.

The case was complicated because the attacks were conducted within the United States with U.S. civilian aircraft. The hijackers used box-cutters to intimidate and neutralize the crews, and then directed the aircraft toward their designated targets. Could this be considered an armed attack against the United States?

If the civilian aircraft were used as powerful guided missiles against U.S. targets with the intention of causing a maximum of casualties, the answer is that this would be an armed attack against the United States. However, the aircraft were American; they did not come from abroad; they took off from U.S. airports.[21]

The first official indication about the identity of the perpetrators of the 11 September attacks was presented to the NATO Secretary General and to the NAC by the Deputy Secretary of State of the United States, Richard Armitage, on 20 September 2001. This was the information necessary to effectively invoke Article 5. Despite Lord Robertson's reiteration of the Alliance's determination to contribute to the campaign in response to the terrorist attacks, the message of the Deputy Secretary of State was clear: "I didn't … come here to ask for anything. I came here to share with good Allies the information we have." [22] U.S. statements and actions made it clear that the campaign would be conducted by a U.S.-led "coalition of the willing"—which also might be called a "coalition of the chosen"—and that NATO would not be expected to play a leading role in the forthcoming operation.

> Washington made it clear that the counterterrorist campaign will be led by the United States, not NATO. "If we need collective action, we'll ask for it," said U.S. Deputy Secretary of Defence, Paul Wolfowitz. Campaign decisions are made in the Pentagon, not in Brussels.[23]

However, the Alliance would have been put in a delicate situation if the invocation of Article 5 were not applied in practice. Most of the measures requested by the United States and adopted by the NAC on 4 October 2001 relate to the provision of support from individual allies. In other words, the United States could achieve a considerable part of the requested support on a bilateral basis: intelligence sharing, blanket overflight clearances, access to airfields and seaports, increased security for the U.S. facilities abroad, etc.

NATO Operations in Support of the Campaign against Terrorism

The most significant collective measures, among the eight adopted by the NAC, are the deployment of seven NATO AWACS aircraft to the United States (Operation Eagle Assist) and the deployment of NATO Standing Naval Forces to the Eastern Mediterranean (Operation Active Endeavour).

Operation Eagle Assist (9 October 2001 – 16 May 2002) was aimed at enabling the United States to use its own AWACS aircraft in the campaign against terrorism, "to enhance NORAD's capability to continue combat air patrol missions and to lower the operational tempo of the U.S. AWACS fleet." [24] In response to the U.S. request and in fulfilment of the NAC decision of 4 October, the NATO Airborne Early Warning and Control Force (NAEW&CF) deployed seven Airborne Warning and Control Systems aircraft (AWACS) to the United States from their main base in Geilenkirchen, Germany. Within the operation, in which 830 crewmembers from 13 NATO nations took part, the NATO AWACS aircraft flew nearly 4300 hours in over 360 operational sorties.[25]

Since the end of Operation Eagle Assist, the NAEW&CF provided airborne surveillance over more than 30 special events, including the funeral of Pope John Paul II in Rome, the Spanish Royal Wedding in Madrid, the 2004 Olympic Games in Athens, Greece, and the European football championship in Portugal, as well as the 2006 Winter Olympic Games in Turin, Italy.

While Operation Eagle Assist had some practical applicability to the campaign against terrorism (relieving U.S. AWACS aircraft for participation in Operation Enduring Freedom), Operation Active Endeavour has had a more symbolic character so far – "providing presence and demonstrating resolve," according to official statements, as noted above.

The eastern rim of the Mediterranean Sea is shaped by the coastlines of Greece, Turkey, Cyprus, Syria, Lebanon, Israel, Egypt, and Libya. While two of these states are NATO members and two are participants in NATO's Mediterranean Dialogue, two other countries, Libya and Syria, are presented in the U.S. State Department's *Patterns of Global Terrorism 2001-2003* as supporters of terrorism.[26] However, both Libya and Syria condemned the 11 September attacks and, in different ways, have recently tried to divest themselves of ties to terrorism.[27] Citizens of Egypt and Lebanon participated in the 11 September suicide terrorist attacks.

On one hand, sending naval vessels to the Eastern Mediterranean could be considered as a warning and expression of resolve against states sponsoring terrorism. However, at that time it was unclear what kinds of operations these ships would be able to perform against diverse international terrorist organizations. The types of ships com-

prising Task Force Endeavour (TFE) differ from those designated to destroy land-based targets. The first STANAVFORMED group participating in Operation Active Endeavour consisted of seven frigates and one destroyer. The primary purpose of such ships is conducting maritime interception activities; and they are armed with ship-to-ship, ship-to-air, and anti-submarine weapons. From present point of view, the main TFE's task has been to present a deterrence posture so as to prevent possible terrorist attacks similar to that against the USS *Cole* in 2000. In practice, TFE has been engaged in monitoring the merchant vessels in the region. In conducting this task, TFE could possibly identify ships illegally trafficking in weapons or immigrants. However, it has not had legal ground to seize such ships; it could only inform NATO and the flag states about illegal activities conducted by these ships. In general, Operation Active Endeavour could be qualified as a maritime interdiction operation.

In March 2003, NATO expanded Operation Active Endeavour by providing escorts to non-military ships from Alliance member states through the Straits of Gibraltar. In April 2003, the operation scope was further expanded to include systematically boarding suspect ships. These boardings take place with the compliance of the ships' masters and flag states in accordance with international law. In March 2004, the operation area of responsibility (AOR) was expanded to cover the entire Mediterranean. At the June 2004 Istanbul Summit, NATO accepted the Russian and Ukrainian offers to support Operation Active Endeavour. Russian ships are expected to join TFE in the middle of 2006.

By the end of February 2006, TFE had monitored more than 75,000 vessels and conducted 100 compliant boardings. A total of 488 vessels had been escorted through the Straits of Gibraltar. Operation Active Endeavour provided also assistance to the Greek government to ensure the safe conduct of the 2004 Olympic and Paralympic Games.[28]

NATO's Engagement in Afghanistan

International contributions to the U.S.-led military campaign in Afghanistan and to the UN-led ISAF achieved significant dimensions. According to the U.S. Department of State, as of June 2002, 69 nations had supported the campaign against terrorism, and 20 nations had deployed more than 16,000 troops to the U.S. Central Command's region of responsibility. The total number of non-Afghan forces in the country was about 15,000, of which 8,000 belonged to U.S. coalition partners.[29]

In fulfilment of the eight measures for expanding the options in the campaign against terrorism, adopted by the NAC on 4 October 2001, the NATO allies provided, both individually and collectively, the following contributions:

- All 19 NATO Allies and the 9 NATO "aspirants" (without the Former Yugoslav Republic of Macedonia and Slovenia) have provided blanket overflight rights, ports/ bases access, refuelling assistance, and increased law-enforcement cooperation.
- 16 Allies now support Operation Enduring Freedom (OEF) in Afghanistan and the global campaign against terrorism. 14 Allies have deployed forces in the region. 9 Allies are participating in combat operations.
- Allies and other partner countries have deployed nearly 4,000 troops to Afghanistan and also provide 95% of the International Security Assistance Force (ISAF), led first by the United Kingdom.[30]

The Afghan Interim Authority took office on 22 December 2001. In order to provide support to the new government and to create conditions for the post-Taliban recovery of the country, on 20 December 2001 the UN Security Council adopted Resolution 1386 to launch the International Security Assistance Force (ISAF) with a peace-enforcement mandate under Chapter VII of the UN Charter. Despite ISAF was established by UN, it was not an UN force. ISAF was manned by the coalition of the willing, supported by NATO, and financed by the troop-contributing nations. The primary task of the force was to assist the Afghan Interim Authority in the maintenance of security in Kabul and its surrounding areas so that the Transitional Authority and United Nations personnel could operate in a secure environment.

NATO first became involved in ISAF in response to a request from Germany and the Netherlands for support in the planning and execution of the third force rotation. In that period, it became clear that the smaller participating countries had difficulties in acting as ISAF lead nations on a six-month rotational basis and providing forces at the same time. On 11 August 2003, NATO took over command of the ISAF with a schedule to continue the operation until 2007. In fact, this was the first Alliance mission beyond the Euro-Atlantic area.

NATO has been increasing its presence in Afghanistan by creating and expanding Provincial Reconstruction Teams (PRTs) in addition to the 14 PRTs acting under Operation Enduring Freedom. These teams, consisting of international civilian and military personnel, work in Afghanistan's provinces to extend the authority of the central government and to provide a safer and more secure environment in which reconstruction can take place. NATO also agreed to deploy extra troops in support of the electoral process in October 2004. At the time of the election, NATO had more than 10,000 troops in Afghanistan, including quick reaction forces both in and out of theatre. Currently, NATO has nine PRTs in North and West Afghanistan and is expanding its presence in south by establishment of four more PRTs.

Despite the fact ISAF is not a counter-terrorism operation, it has a strong impact on international security. In the words of NATO Secretary General Jaap de Hoop Scheffer, "Afghanistan is a top priority for NATO. Our own security is closely linked to the future of Afghanistan as a stable, secure country where citizens can rebuild their lives after decades of war." [31]

Nevertheless NATO has not played a leading role in the campaign against terrorism since 11 September 2001, its support has been vital. In the words of Ian Lesser, "the Alliance played and continues to play a critical consensus-building role. The multinational operations in Afghanistan have clearly been facilitated by the planning capabilities and habits of cooperation developed by the Alliance." [32]

The military role that NATO has had in the campaign against terrorism has been mainly supportive, but the experience that the allies have gained as a result of their common work for decades within the Alliance provides them with a solid basis for effectively participating in military operations outside NATO's chain of command. As Philip Gordon of the Brookings Institution has noted,

> While NATO's formal military role was necessarily very limited in the first weeks of the military campaign, the alliance's political solidarity was highly significant, as is the military interoperability that will allow some allies to participate in later stages of the campaign.[33]

NATO's Political Efforts in Support of the Campaign against International Terrorism

Prague Summit Decisions Related to NATO's Role in the Campaign against Terrorism

At the Prague Summit in November 2002, NATO leaders approved a package of measures to defend and protect their populations, territory and forces from any armed attack from abroad, including by terrorists:

- A new Military Concept for Defence against Terrorism;
- A Partnership Action Plan on Terrorism;
- Five nuclear, biological and chemical defence initiatives: a deployable nuclear, biological and chemical analytical laboratory; a nuclear, biological and chemical event response team; a virtual centre of excellence for nuclear, biological and chemical weapons defence; a NATO biological and chemical defence stockpile; and a disease surveillance system;
- Enhanced protection of civilian populations, including a Civil Emergency Planning Action Plan;
- Enhancement of missile defence capabilities;
- Cooperation with other international organisations;

- Enhancement of cyber-defence of NATO and national critical infrastructure assets, including information and communications systems;
- Improved intelligence sharing.

One of the most important aspects of the Military Concept for Defence against Terrorism is that nations have the primary responsibility for defence of their populations and infrastructures, so the Alliance should be prepared to augment nations' efforts. The Concept outlines four roles for NATO's military operations for defence against terrorism: anti-terrorism (defensive/ passive measures), consequence management, counterterrorism (offensive/ active measures), and military cooperation. The Alliance could either lead or support counterterrorism operations. Most importantly, the Concept defines the possible NATO military role in the fight against terrorism: "NATO needs to be ready to conduct military operations to engage terrorist groups and their capabilities, as and where required, as decided by the North Atlantic Council." [34]

The Partnership Action Plan against Terrorism is the main platform for joint efforts by Allies and Partners in the fight against terrorism. It provides a framework for cooperation and expertise sharing in this area through political consultation and practical measures, such as:

- Intensified consultations and information sharing;
- Enhanced preparedness for combating terrorism;
- Impeding support for terrorist groups;
- Enhanced capabilities to contribute to consequence management;
- Assistance to partners' efforts against terrorism.[35]

Science is another area for cooperation between NATO, Partner- and Mediterranean Dialogue countries in decreasing the terrorist threat. The NATO Security through Science Programme provides opportunities for exchange of scientific and technological knowledge on topics relevant to the fight against terrorism: chemical, biological, radiological or nuclear threats; explosives detection; energy security; information security; social and psychological consequences of terrorism; and analysing the roots of terrorism.[36]

The Civil Emergency Planning Action Plan aims to improve civil preparedness against, and manage the consequences of, possible terrorist attacks with chemical, biological and radiological agents. As a first step, NATO Allies and Partners have established an inventory of national civil and military capabilities that could be made available to assist stricken nations.

The necessity of enhanced missile defence has been determined in response to the proliferation of weapons of mass destruction and their means of delivery, including

missiles of all ranges. NATO is considering by 2010 to have the capability to protect its deployed troops against short- and medium-range ballistic missiles. In this regard, the Alliance is conducting activities in three directions:

- Developing a Theatre Missile Defence (TMD) capability to protect troops, wherever deployed, against short- and medium-range ballistic missiles;
- Examining options for protecting Alliance forces, territory and populations against the full range of missile threats;
- Conducting activities under the NATO-Russia Council to support potential future joint NATO-Russia theatre missile defence operations during crisis response missions.[37]

The international organizations NATO has closer cooperation with in defence against terrorism are the European Union and the UN. The Alliance and the European Union have exchanged civil emergency planning inventories. NATO contributes actively to the work of the United Nations Counterterrorism Committee. There are regular consultations between the Alliance and the Organization for Security and Cooperation in Europe. The Euro-Atlantic Disaster Response Coordination Centre works closely with the UN agencies that play a leading role in responding to international disasters and in consequence management—the UN Office for the Coordination of Humanitarian Affairs and the Organisation for the Prohibition of Chemical Weapons—and other organisations.

Istanbul Summit Decisions Related to NATO's Role in the Campaign against Terrorism

In June 2004, additional measures to increase the Alliance contribution to the campaign against terrorism were approved at the NATO Summit in Istanbul. These measures included: enhanced intelligence sharing, mechanisms for more rapid response to member countries' requests for support in case of terrorist attacks threat, and a research and technology programme of work for better forces' and populations' protection against terrorist acts.[38]

Mechanisms for more effective intelligence information sharing included optimizing the intelligence structures at NATO and more effective use of the NATO Terrorist Threat Intelligence Unit, which was established as a permanent structure to analyse terrorist threats aimed at NATO.

The AWACS fleet, Operation Active Endeavour elements, and the NATO multinational chemical, biological, radiological, and nuclear defence (CBRN) battalion (established in December 2003) were made available to any member country requesting assistance in case of terrorist threat or while hosting major events. Some examples of such assistance were provided above.

When approved, the research and development programme of work included eight major areas for rapid fielding of technology solutions for defence against terrorist attacks:

- Protection of large-body aircraft against man-portable air defence systems (MANPADS);
- Protection of harbours and vessels against surface and underwater threats;
- Protection of helicopters against rocket-propelled grenades (RPGs);
- Countering improvised explosive devices (IEDs);
- Capabilities for precision airdrop for special operations forces;
- Detection, protection and defeat of CBRN weapons;
- Technology for intelligence, surveillance, reconnaissance and target acquisition of terrorists;
- Explosive ordnance disposal (EOD) and consequence management.

In 2005, two more areas were added to the programme: Defence against Mortar Attacks and Protection of Critical Infrastructure.

Post-11 September NATO-Russia Relations

The terrorist attacks against the United States on 11 September 2001 gave a new impetus to NATO-Russia relations. The cooperation in countering terrorism has proven to be of importance to both parties.

Although on 11 September 2001 a new page in NATO-Russia relations was opened, the process of *rapprochement* started after the appointment of Vladimir Putin as Acting President of Russia on 31 December 1999. In March 2000, a meeting of the NATO-Russia Permanent Joint Council was held with an agenda broader than peacekeeping in the Balkans. Since then, despite Western unease with Russia's operations in Chechnya, cooperation has become more intense.[39] According to Martin Walker,

> After September 11, despite the opposition of much of Russia's security establishment, including his old KGB colleague, Defence Minister Sergei Ivanov, Putin agreed to an unprecedented and far-reaching support of Bush's war on terrorism. He ordered Russian Intelligence (FSB) to share information on the Taliban and opened Russian airspace to American logistics aircraft. He overruled the earlier statements of his military establishment to accept a U.S. military presence in Uzbekistan, and helped rearm and equip the anti-Taliban Northern Alliance.[40]

Russian diplomacy seized the opportunity and undertook moves to put Russia and the Chechnya problem in the context of the campaign against terrorism. "[T]he al-Qaida network and the Taliban regime in Afghanistan had long been accused by Russia of aiding and radicalising rebel groups in Chechnya and fomenting instability along

Russia's southern rim. The notion of 'common interests' had never been clearer, on either side." [41]

Russia joined the anti-terrorist coalition and the allies welcomed this step. However, they have chosen to revise their stance toward the Chechen conflict. Apparently for the allies it might be more important to have Russia as a partner than to insist on supporting the various Chechen "freedom fighters." At the NATO-Russia Conference on the Military Role in Combating Terrorism, Lord Robertson stated, "The terrorist threat is not new. Our Russian colleagues, who have seen the tragic loss of countless military and civilian lives at the hands of terrorists over the past decade, can bear witness to that." [42]

At the same event, the Russian Defence Minister, Sergei Ivanov, set forth Russia's conditions for further cooperation in the struggle against terrorism: "If somebody still finds it beneficial to render 'hearty welcome' to representatives of the Chechen terrorist groups… then we state it firmly that all talking about our unity and solidarity may remain 'empty words.'" [43]

Since October 2001, NATO and Russia have launched several initiatives related to the common struggle against terrorism. Some of these initiatives include "regular exchange of information and in-depth consultation on issues relating to terrorist threats, the prevention of the use by terrorists of ballistic missile technology and nuclear, biological and chemical agents, civil emergency planning, and the exploration of the role of the military in combating terrorism." [44] The NATO-Russia Council (NRC), which in 2002 replaced the NATO-Russia Permanent Joint Council, has focused its efforts on the following areas: terrorism, crisis management, non-proliferation, arms control, theatre missile defence, civil emergencies, military cooperation and defence reform, new threats and challenges, and search and rescue at sea.

In June 2002, Lord Robertson outlined the importance of the NATO-Russia partnership as follows:

> Countering terrorism is at the heart of NATO's new relationship with Russia… We need Russia to face new and common threats, just as much as Russia needs us. Russia is now willing to play an honest, cooperative role in working with us.[45]

In that period, the U.S. administration declared a shift in the U.S. position regarding Chechnya and terrorism. On 28 February 2003, the U.S. Secretary of State designated three Chechen organizations as terrorist groups in view of their direct involvement in the hostage-taking at Moscow's Dubrovka Theatre in October 2002. However, the U.S. government stated clearly that it does not consider all Chechen fighters terrorists.[46]

On 7 September 2004, following the series of terrorist attacks on the Russian Federation, the NATO-Russia Council met in extraordinary session. The Council strongly condemned the terrorist acts which caused the death of hundreds of children and other civilians in Beslan, North Ossetia. NATO-Russia Council also declared its determination to strengthen and intensify common efforts to fight terrorism. One of the immediate results was the approval of an action plan to coordinate practical cooperation under the NATO-Russia Council (9 December 2004). The plan aims to enhance Allied and Russian capabilities to act individually or jointly in preventing terrorism, combating terrorist activities, and managing the consequences of terrorist acts.

NATO's Future Role in Countering the Terrorist Threat

In a series of statements, NATO clarified the definition of its future roles and missions regarding the fight against terrorism. On 6 December 2001, the NAC reiterated the Alliance's determination to play an active role in this struggle. In this statement the NAC envisaged some important practical measures related to NATO's future roles and missions for combating terrorism:

> Disarmament, arms control and non-proliferation can make an essential contribution to the fight against terrorism. We will enhance our ability to provide support, when requested, to national authorities for the protection of civilian populations against the effects of any terrorist attack… We reaffirm our willingness to provide assistance, individually or collectively, as appropriate and according to our capabilities, to Allies and other states which are or may be subject to increased terrorist threats as a result of their support for the campaign against terrorism.[47]

On 18 December 2001, NATO declared its resolve to adapt its capabilities to the new challenges to international security. However, in this statement the allies did not assign the military the primary role among the other possible means of countering terrorism:

> [W]e are especially concerned to ensure that the Alliance military concepts evolve in keeping with our clear appreciation of the menace posed by terrorism. Such action must of course make use of a wide range of national and international means, of which military ones are only a part.[48]

On 31 January 2002, in response to critics who argued that NATO has no role in dealing with the new threats, Lord Robertson stated that "the Alliance is becoming the primary means for developing the role of the armed forces to defeat the terrorist threat." [49] This does not mean that the Alliance will become a primary tool for combating terrorism. It means, however, that NATO will provide coordination and a framework for appropriate training of the armed forces for possible anti-terrorist tasks.

On 14 June 2002, Lord Robertson declared some "fundamentally important decisions" [50] made by the NAC that outline the areas in which NATO can contribute most effectively to the fight against terrorism:

> NATO should be ready to help deter, defend, disrupt and protect against terrorist attacks, or threat of attacks, directed from abroad against our populations, territory, infrastructure and forces, including by acting against these terrorists and those who harbour them. Similarly, if requested, we should be ready to provide assistance to national authorities in dealing with the consequences of terrorist attacks, particularly where these involve chemical, biological, radiological or nuclear weapons. We agreed that NATO should be ready to deploy its forces 'as and where required' to carry out such missions. And we agreed that, following a case-by-case decision, NATO might provide its assets and capabilities to support operations undertaken by or in cooperation with the EU or other international organisations or coalitions involving Allies.[51]

However, some analysts have expressed reasonable concerns about significantly broadening NATO's roles in combating terrorism:

> The formulation of a broad response to the challenges posed by transnational terrorism is beyond NATO's capabilities or its appropriate functions. The EU and G-8 have developed an extensive network of inter-agency cooperation in combating transnational crime and subversive organizations; it makes more sense to build on that than to extend NATO into an 'anti-terrorist alliance,' as some have suggested in the wake of the attacks on New York and Washington.[52]

The analysis of NATO's current participation in the campaign against terrorism and the assessment of the appropriate role of the military in combating terrorism and winning asymmetric conflicts suggest key findings about the future possible role of the Alliance in the struggle against international terrorism.

First, NATO has historically concentrated on defence capabilities relevant to its main goal – assuring peace and security in Europe. Most of the European allies do not have significant force projection capabilities and must rely on U.S. assets. The new threats require new responses, including new force structures and new capabilities. However, the new responses also call for new strategies, tactics, priorities, training, and resources.

Second, NATO has developed several mechanisms for reducing the threats posed by the huge stockpiles of small armaments and light weapons in Eastern Europe and the former Soviet republics. It also has politico-military tools for reducing the risk of proliferation of weapons of mass destruction (WMD) through active cooperation with its partners in Europe, Asia, and Africa.

Third, the winning strategy for the strong actor in asymmetric conflict, at least in some circumstances, is to apply the same approach as the weak one. In the case of combating terrorist cells this might mean covert operations, low-intensity conflicts,

surprise raids, and other unconventional methods. NATO forces do not fully meet the requirements for conducting such operations and therefore need additional preparation and equipment.

Fourth, the law-enforcement and intelligence agencies have the main responsibility for countering internal threats posed by domestic and/or international terrorist organizations. In principle, the military should be used only as the last possible option for restoring public order, or as a military support to the civil authorities – for preventing terrorist attacks and/or for dealing with the consequences of possible terrorist attacks, including attacks conducted with WMD.

NATO has to adapt itself to the new international security environment; otherwise, it may become a regional political-military organization with some peacekeeping functions. Currently, the military capabilities of most of the allies do not allow them to rapidly deploy forces far beyond NATO's borders. The forces and assets which the allies are ready to contribute are much more prepared to participate in peace support operations than in high-intensity combat or long-range power projection. The fact that the United States allotted the Alliance a secondary, supportive role during the initial phases of the post-11 September campaign against terrorism has led the allies to redefine NATO's future role in countering international terrorism. NATO has a future role in the struggle against international terrorism, but it must also continue to support the significant non-military efforts to neutralize the terrorist threats.

Conclusion

The Atlantic Alliance's solidarity and the perception of a common threat were the leading factors for the Article 5 implementation. However, NATO as a whole was not prepared to take part in the campaign in Afghanistan. In September-October 2001 the United States had to choose between a NATO-led and a U.S.-led campaign. Some American analysts appear to have perceived it as a choice between the political advantages of NATO-led action and the operational advantages of U.S.-led action. The necessity of fast decisions and rapid action, the military capabilities gap between the United States and the European allies, and the experience from NATO's Operation Allied Force in the 1999 Kosovo crisis defined the United States' decision, in the words of Secretary of Defence Donald Rumsfeld, that "The mission must determine the coalition." [53] That is, Washington chose to lead a coalition of states having the necessary anti-terrorist assets with sufficient sustainability and their own airlift and sealift capabilities.

This decision reveals one of the major problems which NATO has yet to solve: defining the Alliance's roles and missions for the twenty-first century. At this stage contradictions exist between declaring the campaign against terrorism as one of

NATO's main goals and the limited opportunities for realization of this goal. The asymmetric threat that terrorism poses requires asymmetric responses. Massed military power cannot be fully effective against dispersed terrorists who are difficult to distinguish from ordinary citizens. Additionally, since terrorism has both internal and external dimensions, domestic law-enforcement and intelligence agencies bear major responsibilities for dealing with terrorist threats domestically.

In practice, the involvement of NATO as a military alliance in the campaign against terrorism has included sending Airborne Warning and Control Systems (AWACS) aircraft to the United States, sending naval forces to the Eastern Mediterranean to demonstrate NATO's solidarity and resolve, conducting preventive action by NATO's peacekeeping forces against terrorist groups acting within or from the Balkans, and taking the lead of ISAF in Afghanistan.[54]

The scope of NATO's reaction to the 11 September attacks, the characteristics of international terrorism as an unconventional and asymmetric threat, and the relatively small contribution that the military could make in combating terrorism constitute factors that support the main hypothesis of this article: that NATO may be unable to play more than a limited role in the fight against international terrorism. However, the Alliance may yet be able to make greater contributions in preventive and protective functions. The decision to create the NATO Response Force (NRF) was approved at the NATO Summit in Prague in November 2002. It has to achieve full operational capability no later than October 2006. NRF could be used not only for collective defence but also for implementation and enforcement of decisions of the United Nations Security Council directed towards neutralizing threats posed by terrorism.

Notes:

[1] The views expressed in this article are those of the author and do not reflect the official policies or positions of NATO, the Ministry of Defense of the Republic of Bulgaria, or any other Bulgarian institution.

[2]. President George W. Bush, "Address to Joint Session of Congress," in *Patterns of Global Terrorism 2001* (United States Department of State: Office of the Coordinator for Counterterrorism, 20 September 2001), <http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10220.htm> (17 February 2006).

[3] The term *war on terrorism* seems to be imperfect. A war is presupposed to have a beginning and an end. If the end of the war on terrorism is to be marked by defeating all terrorist groups of global reach, this endeavor could be open-ended. Martha Crenshaw argues that "terrorism may be a 'cycle of vengeance,' leading to its self perpetuation." (Martha

Crenshaw, "Decisions to Use Terrorism: Psychological Constraints on Instrumental Reasoning," *International Social Movements Research* 4 (1992): 29-42). In this article, the term *campaign against terrorism* is more applicable.

[4] *Patterns of Global Terrorism 2001*, *2002*, *2003*, <http://www.state.gov/s/ct/rls/pgtrpt/> (17 February 2006).

[5] Colin L. Powell, "Preface by Secretary of State," in *Patterns of Global Terrorism 2001* (United States Department of State: Office of the Coordinator for Counterterrorism, 20 September 2001), <http://www.state.gov/s/ct/rls/pgtrpt/2001/html/ 10220.htm> (17 February 2006).

[6] Martin Walker, "Post 9/11: The European Dimension," *World Policy Journal* XVIII, no. 4 (Winter 2001/02): 1-10, 4.

[7] Walker, "Post 9/11: The European Dimension."

[8] John E. Peters, Stuart Johnson, Nora Bensahel, Timothy Liston, and Traci Williams, "European Contributions to Operation Allied Force: Implications for Transatlantic Cooperation," (Santa Monica, CA: RAND, 2001), <http://www.rand.org/publications/MR/MR1391/MR1391.ch2.pdf> (20 January 2003).

[9] Peters, Johnson, Bensahel, Liston, and Williams, "European Contributions to Operation Allied Force," 26.

[10] American Forces Information Service, "Lessons learned from Kosovo," <http://www.defenselink.mil/specials/lessons/acw.html> (9 January 2003).

[11] Peters, Johnson, Bensahel, Liston, and Williams, "European Contributions to Operation Allied Force," 40.

[12] Lord George Robertson, "Rebalancing NATO for a Strong Future" (remarks at the Defence Week Conference, Brussels, Belgium, 31 January 2000), <http://www.nato.int/docu/speech/2000/s000131a.htm> (6 January 2006).

[13] According to one source, the United States provided 90% of this capability. David S. Yost, "The NATO Capabilities Gap and the European Union," *Survival* 42, no. 4 (Winter 2000-2001), 97-128.

[14] David S. Yost, "NATO's Contributions to Conflict Management," in *Turbulent Peace: The Challenge of Managing International Conflict*, ed. Chester A. Crocker, Fen Osler Hampson, and Pamela Aall (Washington, D.C.: United States Institute of Peace Press, 2001), 104.

[15] Yost, "NATO's Contributions to Conflict Management," 103.

[16] House of Commons Defense Committee, *The Future of NATO*, Seventh Report of Session 2001-2002 (London: The Stationery Office Limited, 31 July 2002), 44.

[17] Tomas Valasek, "The Fight against Terrorism: Where's NATO?" *World Policy Journal* 18, no. 4 (Winter 2001/02): 19-25, 19.

[18] Valasek, "The Fight against Terrorism: Where's NATO?" 19.

[19] Statement by the North Atlantic Council, 11 September 2001, NATO Press Release PR/CP(2001)122, <http://www.nato.int/docu/pr/2001/p01-122e.htm> (21 December 2006).

[20] "The North Atlantic Treaty," Article 5, <http://www.nato.int/docu/basictxt/treaty.htm> (2 January 2006).

[21] It is out of the scope of this analysis to determine what applicability Article 5 might have if the hijackers were Americans but directed from abroad, or if the hijackers were foreigners but directed from within the United States by Americans.

[22] Press Availability: U.S. Deputy Secretary of State Richard Armitage and NATO Secretary General Lord Robertson, 20 September 2001, <http://www.nato.int/docu/speech/2001/s010920a.htm> (2 January 2003).

[23] Valasek, "The Fight against Terrorism: Where's NATO?" 19.

[24] Steve Rolenc, "Tinker, NATO Defend America Hand in Hand," <http://www-ext.tinker.af.mil/pa/archive/20011019/01-NATO_AWACS.htm> (6 February 2003).

[25] Statement by the Secretary General on the conclusion of Operation Eagle Assist, 30 April 2002, NATO Press Release (2002)065, <http://www.nato.int/docu/pr/2002/p02-057e.htm> (3 January 2003).

[26] *Patterns of Global Terrorism*.

[27] *Patterns of Global Terrorism*, 67-68.

[28] "NATO Mediterranean Patrols Board 100th Ship," *NATO Update*, 1 March 2006, <http://www.nato.int/docu/update/2006/03-march/e0301a.htm> (4 March 2006).

[29] "International Contributions to the War on Terrorism," *U.S. Department of State Fact Sheet*, (Washington, DC: U.S. Department of Defense, Office of Public Affairs, 14 June 2002), <http://www.state.gov/coalition/cr/fs/12753.htm> (8 February 2003).

[30] "NATO: Coalition Contributions to the War on Terrorism," *U.S. Department of State Fact Sheet*, (Washington, DC: Bureau of European and Eurasian Affairs, 31 October 2002), <http://www.state.gov/p/eur/rls/fs/14627.htm> (6 December 2005).

[31] "Helping Secure Afghanistan's Future," *NATO Briefing*, January 2005, 1-2.

[32] Ian O. Lesser, "Coalition Dynamics in the War against Terrorism," *The International Spectator* 2 (2002): 43-50, quote on pp.44-45.

[33] Phillip Gordon, "NATO after 11 September," *Survival* 43, no. 4 (Winter 2001): 89-106, 89.

[34] <http://www.nato.int/ims/docu/terrorism.htm> (6 January 2006).

[35] <http://www.nato.int/docu/basictxt/b021122e.htm> (6 January 2006).

[36] <http://www.nato.int/science/about/guide.pdf> 6 January 2006).

[37] <http://www.nato.int/issues/missile_defence/index.html> (6 January 2006).

[38] "Enhanced Package of Measures for Defense against Terrorism", Istanbul Summit Reader's Guide, (NATO, 2004), 55-56.

[39] Willem Matser, "Towards a New Strategic Partnership," *NATO Review* 49, no. 4 (Winter 2001): 19-21, <http://www.nato.int/docu/review/2001/0104-05.htm> (8 October 2005).

[40] Walker, "Post 9/11: The European Dimension," 8.

[41] Paul Fritch, "New Beginnings," *NATO Review* (Summer 2002), <http://www.nato.int/docu/review/2002/issue2/english/analysis.html> (8 October 2005).

[42] Lord George Robertson, "NATO-Russia Cooperation in Combating Terrorism: A Good Idea Whose Time Has Come" (Key note address at the NATO-Russia Conference on the Military Role in Combating Terrorism, Rome, Italy: NATO Defense College, 4 February 2002), <http://www.nato.int/docu/speech/2002/s020204a.htm> (3 January 2006).

[43] Sergei Ivanov, "Role of the Military in Combating Terrorism" (Introductory word by the Defense Minister of the Russian Federation at the NATO-Russia Conference on the Military Role in Combating Terrorism, Rome, Italy: NATO Defense College, 4 February 2002), <http://www.nato.int/docu/speech/2002/s020204b.htm> (3 January 2006).

[44] Press Statement on NATO-Russia Co-Operation in Combating Terrorism, Press Release, 28 January 2002, <http://www.nato.int/docu/pr/2002/p020128e.htm> (3 January 2006).

[45] Lord George Robertson, "Tackling Terror: NATO's New Mission," Speech at the American Enterprise Institute's New Atlantic Initiative (Washington, DC, 20 June 2002), <http://nato.int/docu/speech/2002/s020620a.htm> (22 November 2005).

[46] "Three Chechen Groups Designated as Terrorists," (U.S. Department of State: Office of International Information Programs, 28 February 2003), <http://usinfo.state.gov/topical/pol/terror/03022804.htm> (8 December 2005).

[47] "NATO's Response to Terrorism" (Statement issued at the Ministerial Meeting of the North Atlantic Council held at NATO Headquarters, Brussels, 6 December 2001), NATO Press Release M-NAC-2 (2001)159, par. 6-7, <http://www.nato.int/docu/pr/2001/p01-159e.htm> (10 December 2005).

[48] "Statement on Combating Terrorism: Adapting the Alliance's Defense Capabilities," NATO Press Release (2001)173, 18 December 2001, par.2, <http://www.nato.int/docu/pr/2001/p01-173e.htm> (10 September 2002).

[49] Lord George Robertson, "NATO After September 11" (Speech by Lord Robertson, Secretary General of NATO, to the Pilgrims of the United States, New York, 31 January 2002), <http://www.nato.int/docu/speech/2002/s020131a.htm> (3 January 2006).

[50] Lord George Robertson, Speech by NATO Secretary General Lord Robertson at the conference on "International Security and the Fight against Terrorism," Vienna, Austria, 14 June 2002, <http://www.nato.int/docu/speech/2002/s020614a.htm> (3 January 2003).

[51] Lord George Robertson, Speech by NATO Secretary General Lord Robertson at the conference on "International Security and the Fight against Terrorism."

[52] Anthony Foster and William Wallace, "What is NATO for?" *Survival* 43, no. 4 (Winter 2001): 107-122.

[53] Secretary of Defense Donald Rumsfeld, Remarks on "21st Century Transformation" of U.S. Armed Forces at National Defense University, Fort McNair, Washington, D.C., 31 January 2002, <http://www.defenselink.mil/speeches/2002/s20020131-secdef.html> (10 January 2003).

[54] "Terrorism and the Emergence of New Threats," in *NATO Handbook*, <http://www.nato.int/docu/handbook/2001/hb0106.htm> (24 November 2005).

LTC KRASSIMIR KOUZMANOV is currently serving on the International Staff, NATO HQ, Brussels, Belgium, responsible for coordinating the NATO Programme of Work on the Defence Against Terrorism (POW DAT). His previous professional experience includes assignments in both the Defence Policy Directorate and the former Euro-Atlantic Integration Directorate, Bulgarian MoD, numerous assignments associated with the national defence industry, as well as service with the 9th Armoured Brigade, Bulgarian Armed forces. LtCol Kouzmanov has a Masters degree in International Security and Civil-Military Relations from the Naval Postgraduate School, Monterey, California, a Masters degree in Economics and Organization of Defence Industry from the University of National and World Economy, Sofia, Bulgaria, and a Bachelors degree in Armoured Vehicles Mechanics from the Army Academy, Veliko Tarnovo, Bulgaria.

SPECIAL OPERATIONS FORCES IN THE FIGHT AGAINST TERRORISM ON NATIONAL TERRITORY

Col. Plamen TORLAKOV

Abstract: This article presents basic definitions related to terrorism and examines the essence and main features of this phenomenon, as well as possible targets of terrorist actions. Based on official documents, the author presents the roles and the tasks of the Bulgarian Armed Forces in the fight against terrorism. In the focus of his examination is the employment of Special Operations Forces in the fight against terrorist units on the territory of the Republic of Bulgaria and the support, provided by all national organizations with counterterrorist missions to tactical groups.

Keywords: Counterterrorism, Special Operations Forces, Bulgarian Armed Forces, Ministry of the Interior, Land Forces, Special Antiterrorist Unit, Hostage Rescue Operations.

Introduction

We have witnessed significant changes in the system of international relations in recent years. As a result of the continued intensification of social, demographic and ecological frictions between large community groups, the end of the Cold War did not bring enhancement of security in a global context. The changes in the security environment placed terrorism and organized crime on front pages as major threats to international security. By and large, terrorism remains the only form currently used for achieving political aims through violence.

Particularly acute are the dangers of international terrorism, drug trafficking, illegal arms traffic and other forms of organized crime, which by their sheer scope turn into a global threat to peace. At the end of twentieth century all these combined emerged as one of the most negative consequences of globalization. In its capacity, organized international crime, and the international terrorism in particular, have a global nature. These wide-reaching problems of the day demand international consolidated reaction; their scale, sharpness and destructive power may have—if there are no adequate and timely preparedness, prevention, and response—catastrophic consequences.

INFORMATION & SECURITY. An International Journal, Vol.19, 2006, 85-101.

The events of September 11, 2001 in the United States, the hostage crisis in Moscow in October 2002, the bomb attacks in Tell Aviv, Grozny, Madrid, and London, the Beslan tragedy and many others confirm that international terrorism is the most serious threat to security today. The conditions for terrorist activities considerably improved with the advancement of democratic values, the development of communications and the easier movement of people and money. In order to achieve their aims, modern terrorists have vast financial, communication and human resources and are, possibly, capable of using radiological, chemical and biological weapons with considerable destructive power and huge psychological effect.

In his speech at the NATO-Russia conference in Moscow on 9 December 2002, the then NATO Secretary General Lord Robertson not only recognized, but emphasized the role of the military in the fight against terrorism [1]:

> Many analysts have stressed the importance of non-military tools – freezing terrorist financing; coordinating police work; tighter border controls; better inspection of shipping containers; and improved intelligence sharing. Let there be no doubt – these analysts are right. Non-military tools are crucial to winning this struggle, and to ignore them is to fail in our common endeavour.
>
> But the military, too, must play its part …
>
> NATO should also be ready to act in support of the international community's efforts against terrorism. … To meet these demanding requirements, NATO is taking concrete and immediate steps to modernise our military forces. … NATO is on its way to becoming a much more effective partner in the international community's response to 21st Century threats.

Definition, Essence and Characteristics of Terrorism

From a methodological point of view, it is important to define with maximum precision the essence and content of the term "terrorism." The definition of terrorism is in close relation to its essence as a phenomenon in social life. Thus, the definition and the essence are regarded as an entity. The United Nations took into consideration the problem of the exact and thorough definition of the term "terrorism," which brought about the need of establishing a new Counter-Terrorism Committee.[2] Another reason behind this work is the frequent interference into the practical work of competent services in cases of clearly criminal offences involving murdering or hurting of people, destruction, or crimes committed out of political motives.

Researchers of the phenomenon "terrorism" are unanimous that these activities are criminal acts/ acts of violence, pursuing political goals.

The definition of "terrorism" closely reflects its nature of a social phenomenon, so its definition and essence are indivisible. Different authors and organizations still have not reached a unanimous definition, to be accepted as legitimate in legal theory and

practice. Edward Herman, Emeritus Professor from Pennsylvania's Wharton School of Business, has offered a politically neutral, straightforward definition of terrorism that is difficult to argue with: "the use of force or the threat of force against civilian populations to achieve political objectives."[3] Although quite succinct, this definition addresses the basic issues – the use of violence, civilian targets, and pursuit of political aims. The political motivation and objectives, pursued by the perpetrators of criminal acts, should be at the heart of the definition of "terrorism." Based on the analysis and comparison of various opinions, we adopted an approach in which terrorism is examined as a complicated political and legal phenomenon, founded in attempts to erode the political principles of governance in the states, targets of terrorist activity. Towards the achievement of this goal, terrorists strive to persuade the society that the government is unable to rule the country, to protect their security and the internal order.

Also, based on this first order definition, it is possible to look at terrorism as an international or national illegal, i.e. criminal activity, involving use of violence or threats of violence in order to achieve concrete political objectives and, most of all, to weaken and destabilize existing governments. Generally, this aspect of the definition may be summarized as follows: "Terrorism is a criminal act with political motives."

Approaching the definition of the term "terrorism" systematically, we need to delineate its essential characteristics as a phenomenon:

- Terrorism is one of the forms of organized violence and as such it is a socially dangerous phenomenon. Terrorists direct their activities towards elimination of people who are active, i.e. politicians, other public figures, military lawyers, etc., or to facilities, where usually there are many people or which are socially significant. Additionally, the means used by terrorists usually lead to death, very frequently of innocent citizens, while damage is huge. Denial of the notion of "innocence" is typical of terrorists; they think that everyone belonging to the society opposing them is guilty. With this sort of moral, victims of terrorist acts are frequently innocent people. Terrorists find particularly important syndromes caused by consequences of violence.
- Concrete political and/or ethno-separatist or religious-political aims are pursued through terrorism; the aims of the latter two can be regarded as political so far as terrorists strive to change a government, terrorist-separatists – to tear off territories from the mother-country, while those with religious motivation – to establish a theocracy. The main objective of terrorists is to destabilize or change the political system and the public power in the state of their activity. All researchers on terrorism are unanimous in regard to this aspect of the phenomenon.

- There is trend towards more active ideological motivation behind terrorist acts. The motives of modern terrorist organizations are of ethno-nationalist, anarchic, religious or purely political nature. All terrorist organizations have ideological grounds and a platform, which make them different from one another and determine the direction of their activities. Something typical for their ideological platforms is the presence of extreme and radical ideas, aiming at changing the political system and public order in society and, on the other hand, justifying the use of violence in pursuing radical objectives.
- Terrorist organizations are solidly organized groups, which pursue their political goals using extreme violence or threat of violence. This fact sets the framework for establishing specific mechanisms and principles of preparation for the execution of the terrorist act itself. Terrorists adhere to one important principle in their activities, i.e. strictly detailed action planning, whereupon predicting and assessing different elements of the environment and the impact of eventual changes. On the other hand, the principle of conspiracy and secrecy during planning and executing terrorist acts is at the basis of their activities, even more so since terrorist organizations are illegal groups with non-legitimate social characteristic.
- Terrorist activities rapidly proliferate. Terrorist organizations spread their activity all over the countries in the scope of their political goals, i.e. countries where acts of violence could weaken or destabilize the legal political authority and form of government.
- In their activities terrorist groups seek the effect of mass. For the purpose of achieving cardinal strategic aims, such as the change of political system and government, violence acts are naturally directed to targets of public importance such as buildings, persons, vehicles, etc. On the other hand, in order to shape societal opinion against the legal government, terrorists strive to provoke massive scare among the population in order to prove that the government is not capable of coping with the violence and of ensuring social order and safety. Towards this purpose, terrorists more and more frequently resort to unscrupulous choice of targets of their violence, trying to cause mass destruction and high number of victims, trying to achieve the syndrome of consequences of violence. In other words, terrorism as a phenomenon targets a circle of people wider than the set of its immediate opponents. We even think it would not be an exaggeration to state that terrorism is directed against the entire democratic society.
- The actions of terrorist organizations are systematic. Quite clearly, in order to succeed in reaching such complex variety of objectives terrorist organizations

use violence systematically. This systematic approach is reflected in the planning of terrorist actions, their wide spread, and the pursuit of mass casualties.

- Terrorism is a symbiosis between the high level of terrorists' political motivation and the low level of participation of the population in the political process in the countries where violent acts are carried out. Terrorist acts are executed by small groups which clearly differentiates terrorism from national liberation movements. This differentiation is quite important from a methodological point of view. As a rule, terrorism does not have such a mass nature. On the other hand, liberation movements do not rely on mass destruction and murder. If they use indiscriminate violence, liberation movements would not be distinguished from terrorist organizations. The distinguishing feature of terrorism compared to other forms of political struggle—revolution, war, guerilla warfare, etc.—is the tactic of indiscriminate and unlimited violence, or threat of violence, over individuals or whole communities that fall as accidental victims of circumstances without being directly opposed to terrorists. On the other hand, terrorists usually try to evade direct clash with governmental authorities, such as the police, the military, paramilitary organizations, or special services. National liberation movements are more or less supported by the population (or considerable part of it) of the country where they are active. On the contrary, similar support in regard to terrorist organizations is not observed.

Given its complex and contradictory essence, modern terrorism turns into a social threat. It causes serious problems to internal and international politics and law. It should be noted that terrorists and organized crime groups often use the same methods to exercise their influence and to achieve concrete objectives. However, there is an essential difference between them. It can be summarized in the roots of terrorism, in the goals pursued by terrorists and, last but not least, in the results of terrorist acts, whereupon innocent people fall victim.

The main reason for the rise of terrorism is the rejection of the political system or of concrete political decisions. Usually, this main reason is the external act of a complex of clearly expressed or well-hidden claims of economic, religious, emotional, or social nature.

There are a number of criteria according to which terrorist actions can be categorized, among these are the preferred targets, used means, areas of activity and causes for terrorist actions. According to the ideological reasoning, terrorism can be left-orientated (uttermost left extremism), right-orientated (neo-Nazism, neo-Fascism), religious-nationalistic (ethnocentric, separatist), or religious-political. In regard to target setting, terrorist activities can be subdivided in aerial, maritime, or land. According to the

means used for terrorist acts there are two major groups involving respectively weapons of mass destruction (nuclear, radiological, chemical, or biological) and conventional weapons (explosives, kinetic weapons, etc.).

The structure of a terrorist organization usually includes: leadership, combat groups and support groups. For most of them the number of terrorists is not over one hundred, but there are some exceptions, especially in structures, which operate under the disguise of national liberation movements.

Each terrorist organization has its special features related to the causes of its existence, the nature of its specific goals and tasks, as well as to the methods and means the organization implements. The choice of targets is especially important. It depends on the possible effect, expected reaction, and the accessibility of the target, e.g., the level of its protection. As a rule, terrorists seek and choose "easy" targets, the attack of which would have greatest possible impact.

Roles and Tasks of the Bulgarian Armed Forces in the Fight against Terrorism

Recently, we witnessed an increase of the responsibilities of the Bulgarian Armed Forces (BAF) in the fight against terrorism, weapon trafficking, illegal trafficking of drugs and people and the proliferation of weapons for mass destruction and dual-use equipment and technologies. Challenges are being turned into opportunities. The following activities seem to emerge as priority tasks in preparing BAF for the war on terrorism:

- Creation and introduction of an adequate normative base regulating the use of Special Operations Forces (SOF);
- Enhancement of SOF training, provision of special equipment and significant increase of their mobility;
- Advancing the command, control, communications and information systems in all units of the armed forces;
- Enhancing the medical support system that is to cope not only with acts of bio-terrorism, but also with all contagious diseases that potentially cause epidemics, as well as with scenarios involving high number of fatalities and injuries;
- Building up effective integrated intelligence to ensure timely and precise information on threats; elaboration of new methods of information collection and development of new warning procedures;
- Formulating a national position regarding possible participation in operations against terrorism out of the country's territory; specialization in certain capa-

bilities to provide for effective contribution to counterterrorist operations in the framework of NATO. It is considered that through such specialization BAF will contribute effectively to the fight against international terrorism not only in NATO, but also in the framework of the United Nations and the European Union.

The BAF participation upon occurrence of terrorist acts is regulated in article 68 of the *Law on Defense and Armed Forces*. According to this article, in peacetime, when a "state of emergency" is declared, the armed forces can carry out tasks in support to civil authorities in their fight against the proliferation of weapons of mass destruction, illegal traffic of weapons and *international terrorism*.[4] In addition, article 68 sets the roles of the armed forces as participants in the protection of "strategic sites" and in operations aimed at *interrupting* terrorist acts.

The Ministry of the Interior with its formations has the obligation to perform these tasks. The assumption is that the Bulgarian Armed Forces will be involved only in cases when the capacity of the Ministry of Interior is overwhelmed.

The roles of the armed forces are further elaborated in a set of counterterrorism tasks to be performed by the services:

- The Land Forces assist police units in reporting, blocking, neutralizing and clearing the areas which are targets of terrorism; they support the local authorities with modular units with capabilities to protect the population in cases of ecological crises, epidemics or industrial catastrophes caused by terrorist acts;
- The Air Force conducts observation, reconnaissance and defense of the air space and strategic sites; provides air support to other units of the armed forces participating in the fight against terrorism; provides support to other ministries and state agencies.
- Naval units monitor and protect harbor facilities and navigation devices in order to ensure safety of navigation, military and civilian coastal sites; in case of need, the Navy evacuates civilians injured or threatened by terrorist activities in the area of the Black Sea.

Specifics in the Use of SOF in the Fight against Terrorism on National Territory

The specific features in the use of Special Operations Forces (SOF) reflect the essence and the nature of our actions against modern terrorism. Let us recall three of the points made by the then NATO Secretary General in support of increasing the role of the military in the war on terrorism:

> First, … the clear distinction between terrorism and warfare is fading. Today's terrorists aim to inflict mass casualties, and weapons of mass destruction are increasingly likely to fall into their hands. …
>
> The second reason for an important military role is that the distinction between internal and external security is fading. We used to be able to ensure external security by lining up tanks at the border, leaving internal security to our police forces. We can no longer rely exclusively on that division of labour. Terrorists can slip into our societies, and exploit our openness to inflict massive attacks – attacks that can require the expertise of the military to counter, or that have consequences that only the military can manage. It would be politically absurd not to use every capability at our disposal to deal with this new threat.
>
> Thirdly, there is a military role because it will sometimes be impossible to protect our populations against terrorist attacks using defensive measures only. To prevent a clearly impending attack, or to respond to a successful attack, it may be necessary to deploy military assets offensively against terrorist networks, as in the case of Afghanistan.[5]

Based on that, Lord Robertson made the following conclusion: "… the military has a vital part to play in the comprehensive international campaign to defeat terrorism. The mission of the last century—territorial defence—is out-of-date and out of place. We must radically redefine what the military is to do if we are to meet today's new challenges effectively." [6]

As part of BAF, the Special Operations Forces have some unique characteristics that allow them to perform an important role in counterterrorist operations conducted by the armed forces. SOF units are effective, modular, compact, mobile, combat efficient, relatively independent and sustainable.

All national and territorial police services are directly or indirectly engaged in countering terrorism. Conducting operations for cutting off terrorist acts on the country's territory is the foremost responsibility of the Special Antiterrorist Unit and of the special units of the national services "Fight with Organized Crime," "Gendarmerie," and "Border Police." These organizations, which are part of the Ministry of the Interior, usually react first when there is a signal for terrorist activity and conduct the initial actions for seizing control over the situation.

In the circumstances of an escalating crisis, in order to restrain the crisis and not to allow its expansion, as well as to neutralize terrorist groups of considerable numbers, it is recommended, upon declaring a "state of emergency," to use SOF units without mobilizing all Immediate Reaction Forces of BAF. This is the SOF main role in counterterrorist operations.

When conducting operations of this kind, SOF will fulfill three types of tasks:

- Antiterrorism – defensive measures for limiting the vulnerability to attacks against the population, the territory, the infrastructure and the information and communications infrastructure.
- Preventing terrorist assaults – offensive measures to reduce, prevent, and stop terrorist activities of subversive reconnaissance and terrorist groups.
- Control of the comprehensive set of activities for coping with the consequences of terrorist acts – provision of support to civilian authorities in constraining the impact and stabilizing the situation after such acts.

According to Lord Robertson, in order to accomplish these tasks it is necessary to build up security on the basis of something more than "perfect" plans and reporting diagrams. What we need is capabilities – the right capabilities. Among the priority capability requirements Lord Robertson listed the ability "to move quickly to deter, disrupt, defend or protect against terrorist attacks. With light, mobile forces. With sufficient strategic air and sea lift. With modern command, control, communications and intelligence. And with modern strike capabilities, such as precision guided munitions." It also means having the equipment to detect any use of weapons of mass destruction, as well as to protect the forces operating in an environment where such weapons might be used.[7]

Training is also of paramount importance. There have been occasions when, even though the objective to eradicate terrorism has been well formulated, the use of disproportionate or inappropriate force in the absence of specialized training was ineffective or even counterproductive.

The armed forces should be capable, upon request, to provide assistance to national authorities in dealing with the consequences of terrorist attacks, particularly where these involve chemical, biological, radiological or nuclear weapons. Even more importantly, the armed forces are expected to deal with the threat at its origin. Therefore, as Lord Robertson observed, "military forces of yesterday—huge arsenals of battle tanks, static headquarters and inflexible soldiers—are not only useless in meeting these new threats. They also divert scarce defence resources away from urgent and pressing modernisation. That is simply inexcusable in today's security environment." [8] It is necessary instead to develop quick reaction forces which can be deployed very quickly where needed in order either to carry out an attack or to respond to such attack with a more compact and mobile organization appropriate for the new missions. The build up of mobile, well-trained forces with advanced equipment is extremely important for the war on terrorism in the current security environment. Our military forces should receive proper training to carry out these new missions. They must learn to interact with civilian law-enforcement authorities, to respect the rights

and to secure the trust of civilian populations, to serve not only as combatants, but also as constables and peacekeepers.

SOFs with their specific structure and mobility, with their comprehensive training, with the flexibility in their use, are closest to the above-mentioned requirements as elaborated in the speech of the then NATO Secretary General. SOFs are trained to participate in operations against terrorism, where they are expected to fulfill specific missions and tasks. Therefore, they must undergo a dedicated training in order to understand possible areas of operation, goals and tasks of terrorist organizations and their forces, the ways and the means used by these organizations in carrying out terrorist acts. More specifically, SOF headquarters and units conduct training to perform variety of tasks such as: reconnaissance and detection, pursuing and neutralizing leaders and formations of terrorist organizations; protection of VIPs and strategic sites of national and military importance to the country's security; limiting and isolating threatened areas, protecting the safety and preventing the spread of rumors and panic among the population; direct attacks against the terrorist infrastructure for the purpose of their neutralization or release of hostages.

The antiterrorist operation is a combination of objective-, task-, place- and time-coordinated activities, e.g., negotiations, search and investigative operations, conducted according to a common plan.

There are several types of antiterrorist operations. They may be classified according to the place of the operation, specific features of the participating forces, the time of reaction and the nature of the terrorist act or terrorist actions. We distinguish four main categories of operations:

- Hostage rescue operations are of highest degree of risk. They are conducted after elaborate planning and organization of the interaction among the forces participating in the operation. SOF isolate the area of activity and provide opportunity for the Special Antiterrorist Unit to rescue the hostage;
- Operations, conducted upon the occurrence of a terrorist act, such as securing a building, a vehicle, detonation of explosives, etc. This type of operations is characterized by the short time available for planning. Of particular importance are two additional features:
    - The terrorists have initial advantage as a result of surprise;
    - Wide variety of units with responsibilities for protection of public order or facilities takes part in the operation.

  Depending on the place and time of a terrorist act, SOF can act independently for the elimination of the terrorists, or can block the area till the arrival of special antiterrorist units.

- "Patrol operations" (like those in Northern Ireland, Southeast Turkey, Sicily, etc.) are conducted in areas under the control of "paramilitary organizations" and high terrorist threat. The objective in this type of operations is to restore the control over the territory which is partially (or for a definite period of time) in the hands of the "paramilitary" or terrorist organizations and to provide for normal functioning of the state authorities.
- Reconnaissance-searching operations are conducted in order to localize and capture single terrorists or terrorist groups. Special antiterrorist units and subversive reconnaissance units conduct this type of operations through combination of the methods used by SOF and investigative methods typical for police work.

Main purpose of all counterterrorist operations is the preservation of life and health of people and the defense of national and universal values. A typical characteristic of the antiterrorist operation is the fact that it is carried out under conditions of panic, stress, fear, endangered security, and considerable material losses, while the operation itself consumes tremendous resources.

The antiterrorist operations are conducted according to the following principles:

- *Legitimacy*. Any operation is carried out with awareness of and compliance with the norms of law. Soldiers and staff adhere strictly to legal regulations without going beyond their authority. Bearing in mind the specifics of terrorism, as well as the peculiar sensitivity of international institutions with respect to human rights, it is necessary to comply with the international agreements to which the Republic of Bulgaria is a party. SOF personnel must be familiar with the norms of behavior of the citizens of the country of operation, as well as foreign citizens residing in it. One purpose is that the actions of SOF would not be condemned by national and international courts.
- *Purposefulness*. The ultimate purpose of an operation is to contribute clearly and accurately to the accepted counterterrorist strategy. All subsequent actions follow a unified logic and a strict sequence towards achievement of the endstate, as envisaged in the strategy and provided for in the planning process. In order to combine the efforts of all units participating in the operation towards the achievement of its objectives, it is necessary that all command authorities are duly informed on these objectives through orders or directives.
- *Effectiveness*. The operation is accomplished through clearly assigned tasks; establishment and maintenance of effective communications; realistic assessment of the situation and the factors determining its development; optimum risk assessment and undertaking of adequate actions in response to situation development; avoidance of overlapping efforts through rational interaction;

averting the scattering of resources through formation of mobile reserves of forces and means that would allow to gain control over situations in which the terrorists apply mock activities in an attempt to distract our attention and to spread our forces.

- *Undivided authority*. The antiterrorist operation is to be controlled by a single C2 center coordinating the actions of all participating forces. Operational command centers can be established within the area of the terrorist act, each of these under an authorized person with adequate powers.
- *Security*. Participating personnel is trained and equipped as to provide maximum protection. Security is further enhanced through risk assessment. The purpose is not to allow opportunities to imperil the forces participating in the operation.
- *Support*. Participating forces have the resources adequate for rendering the terrorists harmless and to eliminate the consequences of a terrorist act.
- *Flexibility*. When the situation in the crisis area changes, command authorities and participating forces are able to assess the situation adequately and to react promptly.
- *Mobility*. The C2 authority should have the capability to control the operation directly in the area of the crisis situation. That would assume capabilities to move quickly operational groups and detachments and their equipment, as well as the necessary communications and information systems.
- *Maintenance of permanent readiness of the Special Operations bodies*. Abrupt changes of the situations in the course of the operation are possible. Therefore, it might be necessary to quickly change the decision of the commanding officer in order to achieve the operational endstate.
- *Tactical surprise*. Giving the terrorists an opportunity to predict or decode the activities of the SOF teams can endanger the lives of both hostages and SOF personnel and, at the extreme, to failure of the whole operation.
- *Constant impact on terrorists*. In a hostage situation it is important to maintain permanent contact with the terrorists. That includes psychological and, if possible, visual contact.
- *Concentration of the main forces on the most important targets* (areas of responsibility).

Planning the Antiterrorist Operation

The antiterrorist operation is a higher organizational form of conducting operational and tactical activities by specially trained teams of the Special Operation Forces. It

has two stages – preparation and action. The preparation of the antiterrorist operation in itself has two phases: preliminary preparation – before a terrorist act occurs, and immediate preparation – upon occurrence of the terrorist act.

The preliminary preparation is at the basis of effective counterterrorism. It includes a number of structured activities: obtaining the necessary information; analysis and assessment of possible targets of terrorist acts; provision of support; planning and training.

The collection of information from all possible sources is a decisive factor in determining the level of terrorist threat in a specific area, for a specific site or person. The Special Operation Forces receive such information through regular reports or upon request.

In order to determine the level of terrorist threat it is necessary to have information on:

- Local groups using terrorist methods, including information on their organization, leaders, number of members, specific features, established forms of action, and sponsors;
- External terrorist organizations having interests in the country – control center, structure, specific features and objectives, forms of activity and relations with local organizations;
- Results and analyses of the actions in both successful and unsuccessful special operations against terrorists, especially involving hostage taking, within the country and abroad;
- Domestic and international political, socio-economic or ethno-religious activities and trends that could influence the rise or fall of the terrorist threat.

Analysis and assessment of possible targets of terrorist acts is conducted continuously, with focus on:

- Determining of possible targets, classification of targets according to their importance, determining the level of terrorist threat, defining operational security and protective measures;
- Studying and documenting the technical and tactical characteristics and features of facilities under threat of terrorist acts. Updating, in a timely manner, of the related documentation, i.e., photographs, layouts, maps, blueprints, etc.;
- Developing scenarios (and courses of action) of likely terrorist attacks against the targets, as well as of possible ways of effective counteraction.

In the course of the preliminary preparation of an operation against terrorists, support is provided through preventing or creating difficulties for terrorist activity via implementation of regular counter-measures in three directions: operational-tactical, personnel support, and technical support.

The operational-tactical provision includes the following:

- Clarifying the methods and techniques used by terrorist organizations for collection of reconnaissance information on possible targets, security systems and tactical groups for reaction in case of terrorist acts;
- Constant counteraction to terrorist intelligence through secrecy, disguise, misleading activities, and strict adherence to information sharing and protection measures according to the respective level of classification;
- Avoiding stereotypes in the approach to and the conduct of operations, in particular in the tactical planning of antiterrorist operations and incidents involving hostages.

The second type of support is the support to members of tactical groups and other counterterrorist units. A terrorist threat or attack can be directed against a person or against members of a specific group with or without an obvious reason. The terrorist threat can be demonstrated in a variety of forms – a telephone call, actions aimed at the persons themselves or against members of their family. Therefore, counter-measures are implemented continuously in order to:

- Determine and assess all possible threats, likely places and times of occurrence both in work-related and in family daily routine;
- Identify potential terrorist threats in a building, a car, an airplane or a public facility based on characteristic features or indicators of suspicious behavior;
- Conduct training for protection, counteraction and adequate reaction in the event of a terrorist attack in variety of circumstances and locations;
- Not to permit actions or behavior in everyday life (unless indispensable) that would reveal a person's affiliation with the security forces and tactical groups;
- Consistently use legal means, tactics and techniques for personal protection – from non-disclosure of identity as tactical group members to protective vests, helmets and shields whenever necessary.

Preliminary planning and training are necessary to achieve good coordination of the efforts of various organizations and reliable control over all forces and means that could be used once a terrorist act has occurred. The preparation and the conduct of antiterrorist operations usually involve the state administration at various management levels, security forces and tactical groups. The preliminary planning provides to

the organizations under threat of terrorist attack and the forces expected to react with an opportunity to prepare jointly countermeasures and to carry out a special operation. Thus, each organization is better prepared to exercise control in its area of responsibility and to act according to its internal organizational rules.

Drills and training exercises provide an additional opportunity to coordinate plans for interaction, to enhance command and control, to verify the effectiveness of tactical actions at various levels and, as a whole, to finalize the preliminary preparation of the Special Operation Forces for conducting antiterrorist operations. During this phase personnel and headquarters form the necessary skills and abilities to act in crisis situations. Training is of higher effectiveness when simulated situations and conditions are as realistic as possible.

The phase of immediate preparation is usually shorter; however, it should be comprehensive, covering: organization of the operation, tactical planning, preparation of the forces, deployment in the area of the operation, and organization of the interaction among the participating agencies. This phase starts when the SOF command receives a directive to prepare for actions against terrorists or to assist the structures of the Ministry of the Interior. It is also conducted once a "state of emergency" is announced. Most challenging are the conditions for immediate preparation in case terrorists have taken hostages. The two main reasons may be summarized as follows:

- In order to gain psychological superiority the antiterrorist operation must begin no later than two to four hours after the terrorist act;
- Often terrorists place time-related demands immediately after taking hostages. Such ultimatums have most serious, often fatal consequences and the timely reaction may be critical.

The Special Operation Forces would rarely act alone in conducting an antiterrorist operation.

The control of the antiterrorist operation is based on continuous collection of information on the situation and the condition of the terrorists, the course of the tactical actions and the results achieved, the assignment of additional tasks in changes of the situation, the establishment of conditions for good interaction among participating forces.

The conclusions drawn from the large-scale terrorist acts in the United States and the Russian Federation raised the issue of clear and accurate distribution of responsibilities and powers among the central executive powers and the local administration to make decisions in the course of an antiterrorist operation. Another set of questions addresses the adequacy of intelligence and counter-intelligence capabilities of national security systems, the establishment of a dynamic legal base for managing forces

and other executive organizations, as well as the development of procedures for effective coordination and interaction among these organizations.

Conclusion

The current global security environment and the trends in its evolution provide sufficient grounds to assume that the role of the UN and NATO in resolving conflicts and managing threats to the world peace and security will be increasing.

The tragedy of September 11 turned into a fiasco for all special services and signified a serious breakthrough in the immune system of the democratic world. Pursuing their goals, the terrorists actively use the achievements of civilization and democracy—technological, information, political, financial, juridical—and in many cases more efficiently than the forces expected to counteract them.

A new, higher level of international cooperation is necessary, and Bulgaria is an indispensable part of the international response to terrorism. This country's contribution to the fight against terrorism will be growing in the years to come. The integration of the Republic of Bulgaria in the global coalition for stability, democracy and prosperity and its active participation in peace-keeping operations and the war on terrorism is motivated by the values that we share and the goals that we have – effective membership in NATO and the EU. This is the guarantee and the environment that will make our capacity greater and our contribution – more significant and more efficient.

Notes:

[1] Lord Robertson, NATO Secretary General, "The Role of the Military in Combating Terrorism" (Speech at the NATO-Russia Conference, Moscow, 9 December 2002), <http://www.nato.int/docu/speech/2002/s021209b.htm> (19 Nov. 2005).

[2] For details refer to the Committee's website at http://www.un.org/sc/ctc/ (20 Nov. 2005).

[3] See for example Mark Weisbrot, "A War against Civilians?" *Common Dreams News Center* (2 November 2001), <http://www.commondreams.org/views01/1102-10.htm> (19 Nov. 2005).

[4] Law on Defense and Armed Forces, *State Gazette* (December 1995), latest amendment as published in *State Gazette* 38 (May 2005). This particular text was amended in 2000.

[5] Lord Robertson, "The Role of the Military in Combating Terrorism."

[6] Lord Robertson, "The Role of the Military in Combating Terrorism."

[7] Lord Robertson, "The Role of the Military in Combating Terrorism."

[8] Lord Robertson, "The Role of the Military in Combating Terrorism."

Colonel **PLAMEN TORLAKOV** is Commander of the 68th Special Forces brigade in Plovdiv, Bulgaria. He is a graduate of the "Vasil Levski" Military Academy in Veliko Tarnovo (1982), the Command and Staff course of the "G.S. Rakovski" Defense and Staff College in Sofia, Bulgaria (1991) and the "General Staff" course of the same college (2003). He has served in a variety of command position in the Special Operations Forces. His distinguished military career includes service in the G2 Directorate of the Army Headquarters (1995-1999); Head of the Special Operations Directorate at J-2, General Staff of the Bulgarian Armed Forces (1999-2000); Head of the Special Operations and Electronic Warfare Directorate of the Army HQ.

TERRORISM ON THE SEA, PIRACY, AND MARITIME SECURITY

Bojan MEDNIKAROV and Kiril KOLEV

Abstract: Analyzing sea terrorism and its influence on maritime security, the authors reveal the main sources of this phenomenon, its character and strong connection with piracy. The article examines major tactical forms, ways and methods used by sea terrorists and the necessity to adapt the system for education of maritime personnel.

Keywords: International Terrorism, Terrorism at Sea, Maritime Security, Maritime Transport System, Piracy, Tactical Forms, Education of Maritime Personnel.

In the beginning of the 21st century the world faces new challenges in the field of security. It appears necessary to give a new meaning to contemporary risks and the entire approach to security. It is impossible to guarantee the security only through military means. In the interest of security, it is necessary to use the wide spectrum of political, economic, military and information instruments in order to counteract the variety of risks and threats.

International terrorism is the threat most difficult to eliminate. It has worldwide importance, widens its relationship with organized crime, uses its financial resources, and unites the potential of its personnel with religious fanaticism. Technologies allow terrorists to use gaps in the protection of industrial production to access radioactive materials, as well as to create chemical and biological weapon.

Strategy of the modern terrorism includes:

- Waging psychological war trying to demonstrate the weaknesses of nations regardless of their economic and military potential;
- Declaration of religious wars to provoke conflict between civilizations and to conceal terrorist into religious aims;

- Spreading chaos into the world economy, breaking up the trust in most developed industrial nations, increasing instability of Islamic and democratic governments;
- Creation of mass panic by using biological and chemical toxic materials, provoking feelings of helplessness;
- Threatening computer and communications systems;
- Provoking serious problems in tourism, insurance businesses, transport communications, etc.

The asymmetric character of the terrorist actions allows causing huge material and other damages using fairly limited material and human resources. In addition, among the targets of terrorist attacks are objects of a symbolic character. In some nations, destroying such objects often has considerable public impact and wide international resonance.

Main cause for terrorism is the partial or complete rejection of the existing political system. The terrorism is an external act of clearly shown or disguised political claims with economic, religious, emotional, psychological and social character. Thus, 21st Century terrorism closely resembles some aspects of the anti-globalization movement.

Maritime terrorism is one specific expression of international terrorism. The first serious occurrence of maritime terrorist actions is the hijacking of the Italian passenger ship "Achille Lauro." This capture was carried out by a battle group of the terrorist organization "Front for Liberation of Palestine" in the Eastern Mediterranean in 1985.

The vulnerability of the military and commercial shipping to maritime terrorism was shown during the attack by the fighters of Al Qaeda against USS DDG "Cole" on October 12, 2000. This is not the only incident when the organization of Bin Laden carried out terrorist actions at sea against the USA. In 2000, of the coast of Yemen, the fighters of the organization captured a boat in order to execute attack against the USS DDG "Sullivans." They did not succeed. The boat was overloaded with explosives and nearly sunk. In 2002, again in Yemen's territorial waters, a boat used by terrorists detonated the French oil tanker SS "Limburg."

Bin Laden and businessmen, who share his ideas, own shipping companies. The companies execute illegal commercial operations used to finance the terrorists. Also in 1998, one of Al Qaeda ships delivered a great amount of explosives to Africa. Later, parts of these explosives were used in the attacks against the U.S. embassies in Kenya and Tanzania. Given sufficient amount of money, it is not difficult to turn a

civil vessel into a semi-military one. At one point, Bin Laden spread the message that the "Al Qaeda Navy" includes 20 "naval" ships.

With the attack against the USS DDG "Cole" the terrorists aimed to provoke fear, anxiety and painful reaction in the US society. It is believed that following the example of "Al Qaeda" some Asian and Middle East terrorist groups also prepare to carry out such attacks.

On October 23, 2000, boats steered by volunteers-kamikaze from the group "Tigers for the Liberation of Tamil Eelam" destroyed a Sri Lankan naval ship and damaged another one. This terrorist organization has a subdivision called "Sea Tigers." Periodically, groups from this subdivision carry out attacks against the Sri Lankan Navy. In one of the strikes in 2001 both sides participated with total of 18 ships. In this particular strike the Sri Lankan Navy lost three patrol boats.

On 7 October 2000, a boat steered by the volunteer-suicides from "Hamas" exploded in advance, thus causing only negligible damage to an Israeli naval ship.

Bulgaria, as a sea nation, often faces problems related to maritime terrorism. The list of accidents with ships, sailing under Bulgarian flag, or vessels under foreign flag with Bulgarian crew, is very long. Terrorist and related acts are being carried out today and have happened before. They are carried out at sea, far from Bulgarian territorial waters, but also in the rivers and in our ports. Among the examples are the 1994 hijacking of the river oil tanker "Khan Kubrat," sailing under Bulgarian flag along the river Danube; the explosives found on the passenger ship "Balkan Princess" in the port of Rousse in October 2002; and the attack against the French oil tanker "Limburg" with Bulgarian crew in the territorial waters of Yemen in the same year. Incidents of pseudo-terrorism on the motor ship "Elena" and pseudo-piracy on the motor ship "Aquarius 1" deserve to be mentioned, too.

The maritime terrorism is seen as a combination of illegal actions that affect—directly or indirectly—the interests of a nation at sea or on land. These actions may be grouped into several main categories: piracy, robbery, assaults, hijacking, and illegal trafficking of weapons, people and drugs.

The origins of maritime terrorism are connected to piracy. The piracy is an old crime with international character. Roman law identifies pirates as the enemy of society – *Pirata hostis generis humani*. The international character of pirates' attacks in the remote past is identified by:

- Protection from several nations;
- Lack of respect for sovereign rights stemming from internationally acknowledged borders and flag nation; or

- Avoiding persecution using water areas controlled by a third nation.

There are different forms of piracy, for example maritime and coastal piracy, capers and corsairs. This crime exhibits significant stability. It not only survives, but evolves and sometimes even leaves behind public development. In the middle Ages pirates created their own quasi-state organizations with democratically elected governing bodies in accordance with precise rules. During the times of great geographic discoveries pirates were discoverers and conquerors of new lands.

In the Twentieth Century, piracy kept its place together with other acts of international organized crime. Fighting piracy is a public task. Hence, the 1958 Geneva Open Sea Convention defined ways to fight against piracy.

After the end of the Cold War terrorism and piracy continue to be a well-known phenomenon in many regions of the world. The disintegration of the bipolar political model and changes in the value systems led to the moral collapse in some social groups in the Eastern European nations. Processes of conversion and chaotic reforms in the armed forces and the intelligence services left jobless a great number of highly qualified personnel from defense and intelligence services, Special Forces and others. Moral collapse and economic crisis gave grounds for personnel with special skills to join the criminal contingent. The perfect organization and maritime training of the Somalia pirates makes viable the thesis that many among them are former coastguard officers and professional seamen.

Such circumstances facilitate 'partnerships' between partisan-terrorists and organized criminal groups. Partisan and terrorist groups have developed symbiotic links to organized crime in order to finance their activity. Thus, western democracies are confronted with the challenge to identify precisely the new enemy at sea.

Solutions of the problems of terrorism at sea and piracy are sought in the framework of the declared total war against terrorism. Many areas of the world ocean are proclaimed dangerous for shipping because of high level of pirate activity. In accordance with data of the International Maritime Bureau (IMB) in London, the number of pirate attacks on merchant vessels for the last decade tripled.[1] During the period from 1998 until 2002, 1228 pirate attacks were carried out.

In the beginning of 2005, reduction of the number of pirate attacks was observed in comparison with the same period of the previous year (182 attacks for the period of January–June 2004 and 127 attacks for the period of January–June 2005). Attacks are often carried out in the area near the Somalia seacoast, the Straights of Malacca – the busiest sea area in the world with more than 50 000 passing vessels per year, South China Sea, the waters near port Cochin in India. 92 vessels were attacked and 192 crew members were captured.

Experts identify dry cargo ships and tankers as main targets of modern sea piracy. At the same time, hijacks of tugboats and hydrographic ships are also on the increase. Most vulnerable to attacks are vessels situated on the roadstead or in quay. There are many attacks against the sailing vessels.

In the IMB report on pirate attacks in the first quarter of 2003, ship owners and masters are warned to be extremely careful in planning for and passing through a number of areas, including coastal waters, straights, roadsteads and ports of[2]:

- Southeastern Asia and the Indian subcontinent (Bangladesh, India, Indonesia, Malaysia, Thailand, Vietnam, Philippines, Straight of Malacca);
- Africa and the Red Sea (Conakry, Dacca, Dar es Salaam, Lagos, Aden gulf, the area near the Somalia seacoast);
- South and Central America, Caribbean (Brazil, Columbia, Dominican Republic, Ecuador, Guyana, Jamaica, Peru, Venezuela).

The first two regions are largely covered by the so-called 'strategic triangle.' The strategic triangle includes three main regions: the Persian Gulf with approximately 65 percent of the world oil reserves, the Caspian Sea and Eastern Asia. These regions provide for 49 percent of present-day output and 75 percent of oil reserves. These resources trigger conflicts between many national, regional and international interests.

The definition of exclusive economic zones in the UN Convention on the Law of the Sea leads to disputes among nations regarding their sea boarders. These are particularly severe in key regions, such as Persian Gulf, the Caspian Sea and South China Sea. There is a direct connection between the conflict of interests and limited or complete lawlessness. The lack of law and law enforcement mechanisms contributes to the increase of terrorist activity and means and methods in these regions.

The most dangerous maritime region is the area near the Somalia seacoast with a length of 3000 km and distance from a coastal line of 300 km.

The regions with high concentration of pirate actions are identical to the regions of increased terrorist activity. According to the experts, the pirates in Indonesian waters and especially those acting in the Straight of Malacca are under Al Qaeda's influence. Terrorist formations also carry out pirate attacks in order to receive funding for their main activity. There is a personnel transfusion from the criminal to the terrorist direction. Pirates are often employed by terrorists to execute special political orders.

Terrorists and pirates possess faster boats, more fire power and safer communications than many of the governments in the region. Their attacks become more intensive and more effective, often causing higher number of casualties. These attacks affect negatively navies, coastguard organizations, navigation, and whole societies. Among the

targets of terrorist attacks are vessels, port facilities, and equipment. Damages caused by maritime terrorism to the international market of cargo shipping are estimated in billions of dollars, not including fear and other psychological effects on the citizens.

Pirates cooperate actively with other criminal groups, especially those involved in illegal trafficking of drugs, weapons, and people. It is possible that pirates and other criminal organizations possess not only modern surface vessels, but also submarines. In the 1990s, Columbian drug merchants tried to build a submarine. During the same period, the US intelligence services prevented the sale of Russian submarines to Latin American criminal groups.

The analysis of modern maritime terrorism reveals a pattern – attacks at sea are carried out primarily in developing nations; about 90 percent of the attacks in the last three years. The governments of these nations are often corrupt, ineffective, incompetent and do not have the resources to counter effectively this threat. Governments do not have intelligence services, normative documents and diplomatic influence necessary to destroy terrorist and criminal organized groups. Only drastic governmental reaction against the threat of terrorist and pirate attacks could lead to the liberation of nations from the grip of the organized crime.

First prerequisite for effective reaction against the new threats is to identify correctly their specific features and origin. Maritime terrorists apply wide range of forces and means ranging from land groups trained to put improvised explosive devices on board of vessels to swimmers; fast attack boats; boats, steered by volunteer-suicides and sea mines.

According to their targets, terrorist attacks can be divided in the following categories:

- Attacks against vessels on the sea;
- Attacks against vessels in ports and at anchor, and
- Attacks against port facilities and other coastal targets.

The tactics of maritime terrorists depend on the type of the vessel, which is attacked, the value of the target, the security system of a port, the motives and operational experience of the terrorist group, etc. For example, terrorists often attack merchant vessels. Fighting swimmers are used only against immobile vessels. Fast boats are used both at high sea and near the coast (which makes them a very valuable asset; therefore, terrorist groups try hard to gain access to such boats).

Terrorists try to use the factor of surprise, which is transformed into a special element of their attacks. Terrorists prefer to carry out their attacks on vessels and port facilities in weakly protected ports. The direction of the attack is chosen depending on the weak part of the protection – it may be carried out both from the sea and from the

coast. In well protected ports, terrorists usually concentrate their efforts only in one direction; it is possible though that terrorists choose to attack simultaneously from the sea and from the coast.

The pirate attacks, according to IMB, are of three main types.[3]

The first type of attacks is carried out by small maritime groups. They use fast boats to organize an ambush in waters of busiest sea routes. According to the "outer estimate" of the target, pirates determine the possibility that there is valuable cargo on board and susceptibility of the target to attack. After embarking the vessel, the attackers' goals are money in the ship's safe, valuable private possessions of the crew members or ship inventory. Expropriated possessions are transferred to pirate's fast boats. Usually, the duration of such an attack is between 30 and 40 minutes. The attackers often use violence; as a result crew members may be wounded and even killed.

During such incidents, the vessel under attack is not under the command of its crew for an extended period of time. Seamen are distracted partially or entirely from performing their professional duties and this causes potentially the gravest consequences. In some cases, the movement of supertankers during an attack is controlled only by automatic pilot, while the attack is carried out in canals, straits or other areas with busy navigation. This increases the risk of collision or stranding the ship with all resulting economic losses and grave ecological consequences.

Attacks of this kind are being carried out in the coastal waters and ports of Indonesia and the India subcontinent, West African ports, South America near Brazil, Ecuador and Columbia.

Other attacks target appropriation of the cargo and, occasionally, the vessel. Attacked crews have been killed or left to the mercy of fate in safe boats. Pirates rename a vessel and change the flag. The vessel is diverted to a port chosen in advance, where the appropriated cargo is unloaded and sold. Such attacks are well-resourced; the pirates are determined and relentless. Hijacks of vessels have often happened in coastal waters of Indonesia, the Straits of Malacca and the India subcontinent.

A third type of attacks is typical for the coastal waters of Somalia. The attacks are carried out by representatives of local paramilitary formations. Pirates kidnap members of the crew and seek ransom for their release. When a ship moves slowly or stops, e.g., due to failure of the main engine, in this area of Somalia coast, there is a high possibility that the vessel and the cargo will be hijacked or the crew – kidnapped. For example, in September 2005, pirates from Somalia captured three cargo ships of the Kenyan shipping agency "Motacu" transporting UN humanitarian aid for the population. Often pirates request ransom for ships, their crews and the cargo. One

of the most arrogant attacks took place on November 5, 2005. At about 150 km off the Somalia coast two pirate fast boats reached the passenger ship "Seaborn Spirit" with approximately 300 passengers on board. The attackers launched grenades and used automatic guns. One crew member was wounded. The ship crew used a device that imitated the noise of gunfire, and successfully repelled the pirates. On the next day, a dry cargo ship, sailing in the same area, was attacked by several boats with grenades and automatic small arms. The ship was diverted by pirates who used sharp increase of speed. In the last six months of 2005 alone, 25 pirate attacks were carried out in the waters of Somalia sea coast.

The rise of terrorist and pirate attacks triggered a process of analysis and reassessment, reflected in the activity of the International Maritime Organization (IMO).[4] The 83rd Session of the Law Committee of IMO, 8–12 October 2001, set as main task for 2002–2003 the revision of the International Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SULA–88).[5] In February 2002, the 22nd Assembly of IMO passed Resolution A.294 (22) and formed a Working Group on Maritime Security at the Maritime Security Committee (MSC). The group recommended changes in the international regulations for commercial navigation. Its recommendations address, *iter alia*, organizational and methodological aspects of the specialized training of command and other personnel in formulating and implementing ship security plans. These recommendations were transformed into resolutions at the Diplomatic Conference of Maritime Security held in London in December 2002.[6] The conference passed the *International Ship and Port Facility Security Code* (ISPS Code) and amendments in the *International Safety of Life at Sea Convention* (SOLAS–74). One major change was the addition of a new chapter XI–2 in SOLAS–74 under the title "Special measures to enhance maritime security." [7]

The analysis of these changes allows us to draw the following main conclusions:

- The international dimension of the problems with the security of the maritime transportation system (MTS) has increased in importance. Maritime nations enhance their cooperation in accordance with the regulations of the IMO Diplomatic Conference;
- The responsibility of each country for the security of and the support to civilian vessels sailing under its flag, as well as for the security of vessels sailing in its territorial waters increases;
- The concept of maritime security covers moving and immobile objects, subdivided according to the level of their required protection;
- The concept of maritime security is comprehensive and covers all threats to the safety of navigation.

Changes in the regulatory framework and the results of our analysis guide the preparation of all governmental institutions, maritime and port administrations, ship owners and shipmasters of civilian vessels for implementation of the assumed duties. Of highest importance is the creation of the national legal and administrative base necessary to support the full and effective implementation of the security requirements as defined in chapter XI–2 of SOLAS–74 and the ISPS Code.

Each IMO party implements a number of activities in this regard:

- Seek a consensus among governmental agencies on international agreements on maritime security and report the stance to IMO;
- Create a national organization with responsibilities for the realization of the policy on the security of port facilities security and the communication between a port and a vessel. Seek mutual acknowledgement of national maritime security organizations while enhancing the capacity for management and control of their activities;
- Define the threats to the security of civil vessels and ports, establish the necessary security levels, and publish instructions and security guidance;
- Define precisely the term "port facilities" and nominate a security officer, responsible for planning and realization of the plans for security of port facilities;
- Define points of contact for all civil vessels that use or intend to enter the territorial waters of the country and exchange information on security levels;
- Test and ratify ship security plans and port facilities' security plans; upon ratification, amend existing plans accordingly;
- Oversee the realization of the requirements of Chapter XI-2 and part A of the ISPS Code by all vessels sailing under national flag, as well as by all national port facilities; Provide for acceptance of international security certificates awarded to ships and port facilities;
- Provide the necessary IMO information to other interested parties in accordance with the regulations;
- Inform other interested parties about the prescribed security level of the port facilities and ships that are in or intend to enter the territorial waters of the relevant nation;
- Implement measures necessary to prevent the revealing of information related to security rating of ships and port facilities and their security plans, as well as cases of penetration in the maritime security command and control system.

The IMO convention places high demands on the protection of ships, ports and security-related port facilities through a set of procedural and technical measures. It is

recommended to use equipment with signaling and documentation functions for protection of the access to the most important—in terms of security—zones on ships, ports and port facilities.

Procedures and practices of operational control need to adhere to international and national legal norms with respect, where appropriate, to specifics of culture and religion. There are two important issues in that regard:

- Provision of respect to and protection of national economic and political interests, while guaranteeing the security of maritime communications in the region;
- Implementation of humanitarian-assistance measures in accordance with the requirements of the international legislation for protection of human life on the sea.

On its behalf, NATO has also launched a set of maritime security enhancement measures within the doctrine for *Naval Cooperation and Guidance for Shipping* (NCAGS).[8] The doctrine describes requirements and procedures for military support, NATO guidance and control in the interests of security of the increasing trade shipping in the World Ocean, support of the military operations for protection of shipping in peacetime, in situations of tension during crisis, as well as in conflict situations. It includes different levels of consultative support and control of merchant shipping. The doctrine necessitates military coordination in a few situations of high intensity conflict.

The NCAGS organization includes the following components: theater command; operational formation; control coordinator; groups for control, including liaison officers; command of convoy service and convoy naval forces.

Planning in the regional NCAGS system is carried out by the relevant commander and headquarters. In the planning process, planners are expected to define clearly:

- Boarders of the region, where the NCAGS system deploys;
- Zones, dangerous for shipping in the region with the increased possibility of incidents;
- Points, as well as approaches, for shipping support and control (NCAGS shipping points);
- Location of the regional command and coastal and sea control groups;
- Convoy naval forces – location, optimal size and structure;
- Recommended routes and courses for shipping in the region;
- Beginning of the mobilization of the control system;
- Beginning of system deployment;

- Duration for its activation;
- Maximum number of passing vessels per standard time period (hour, day, week, year) for all recommended routes.

NCAGS is carried out in two phases.

In the first phase, indirect control is exercised through a set of general advice and recommendations to all users. Messages containing information on possible incidents in a region, risk zones for shipping, and recommended navigation routes are transmitted to sailors. This phase begins prior to the activation of the regional system. It is realized mainly through exchange among the Navy, governmental maritime authorities and ship owners. In accordance with the decision of the regional command, complete or partial mobilization of the NCAGS system is carried out.

In the second phase of an active control, the NCAGS system is deployed. Ship masters receive obligatory directives; liaison officers accompany ships, and, potentially, the convoy service is deployed.

In critical areas (areas with possible illegal traffic of people, drugs, weapons and danger of terrorist attacks), the regional NCAGS system has several important advantages: capability for rapid and inexpensive adaptation to the existing infrastructure and the characteristics of the theater; relatively small amount of forces and means in comparison with the convoy system; maximum number of passing vessels per standard period of time and comfort for the ship owners; flexibility and adaptability to littoral waters and neighboring seas; universality for both peacetime and time of war; and high effectiveness.

The realization of the NCAGS system requires development and signing of an agreement for creation of regional structures for solving security problems in a specific region of the ocean or the sea; agreement for reciprocal exchange of security information between governmental institutions of the neighboring sea nations; agreements for organization of multinational formations and rules of engagement in pursuing and destroying civil vessels, perpetrators of terrorist actions or any other vessels carrying out illegal activities on the sea.

All recent changes in the threats, the international and national activities in preparing to meet the new threats, place new demands to the system for maritime security education. Educational institutions are not yet ready to fully satisfy these requirements. The security problems are not yet adequately presented in curricula or in specialized educational disciplines.

The training of the naval specialists and seafarers to counteract maritime terrorism and pirate activities should correspond to planned objectives and functions. No one

expects the crews of merchant ships to solve all problems related to neutralization of terrorists. The goal is to provide training for necessary skills and adequate reaction. This reaction should create capabilities to resolve the following complex problems [9]:

- To prevent a terrorist act;
- To protect life and health of crewmembers and passengers, as well as their release (if necessary);
- To support special force units neutralizing terrorists;
- To protect the ship and its cargo.

Terrorist activity on the sea has global impact. Maritime terrorism is manifested as a many-sided and complex threat against regional security. At this stage, governmental maritime authorities and Navies in some nations are not adequately prepared to execute functions of protecting shipping against maritime terrorism. In these circumstances it is necessary to improve the training of maritime specialists in countering such criminal actions.

Notes:

[1] ICC International Maritime Bureau (IMB), <www.iccwbo.org/ccs/menu_imb_bureau.asp> (21 Dec. 2005).

[2] ICC International Maritime Bureau.

[3] International Maritime Law Institute (IMLI), <www.imli.org> (21 Dec. 2005).

[4] International Maritime Organization (IMO), <www.imo.org/home.asp> (21 Dec. 2005).

[5] Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SULA-88).

[6] International Maritime Organization (IMO): Maritime security is considered an integral part of IMO's responsibilities. A comprehensive security regime for international shipping entered into force on 1 July 2004. The mandatory security measures, adopted in December

2002, include a number of amendments to the 1974 *Safety of Life at Sea Convention* (SOLAS), the most far-reaching of which enshrines the new *International Ship and Port Facility Security Code* (ISPS Code). The ISPS code contains detailed security-related requirements for governments, port authorities and shipping companies. Some of these are mandatory (described in Part A); others, presented in Part B (non-mandatory section) provide guidelines about how to meet these requirements.

[7] *International Convention for the Safety of Life at Sea (SOLAS)*, 1974, Entry into force: 25 May 1980 (International Maritime Organization, last amendment May 2006), <www.imo.org/Conventions/contents.asp?topic_id=257&doc_id=647>.

[8] ATP-2(B) Volume I, *Naval Cooperation and Guidance for Shipping – NCAGS*, NATO. For a national example see Admiral Sir Jonathon Band, "Fighting terrorism on the oceans," *ENVision* 3 (2002), <http://www.manw.nato.int/manw/pages/update/envision_3_02/terrorism.htm>.

[9] International Maritime Law Institute.

BOJAN MEDNIKAROV is Deputy Commandant of the "N.Y. Vaptsarov" Naval Academy, Varna, with main responsibilities for education and research. He has experience as a commanding officer of fast patrol boats and operational officer in the Operational Department of the Navy Headquarters. Since 1995 he is in the educational field as lecturer, head of department in the Naval Academy and at the "Rakovsky" Defence and Staff College in Sofia. His current rank is Captain in the Navy. Dr. Mednikarov is 1984 graduate of the Naval Academy with a major in navigation and 1992 graduate of the "Kuznetsov" Naval Staff College in St. Petersburg, Russia. He received a PhD degree in systems and control in 1999. Since 2000 he is associate professor in the "N.I. Vapzarov" Naval Academy and the "G.S. Rakovsky" Defence and Staff College. Among his research interests are studies of military systems, modelling of the activities of navy units and studies of naval organizations. *E-mail*: bob_mednikarov@abv.bg.

KIRIL KOLEV is a Captain (ret.) in the Bulgarian Navy, born on 27th of October 1955 in the city of Veliko Turnovo, Bulgaria. Currently he is lecturer in the Naval Academy in Varna. After graduating the Naval Academy he served at the Bourgas naval base as executive MCMS officer, operational MCMS officer, MCMS deputy commander, deputy commander of a MCMS group and the chief of staff of the MCMS division. After that he studied in the Naval Staff College in St. Petersburg. Upon graduation Capt. Kolev served as an operational staff officer and head of staff subdivision of the naval base of Varna and, later, as a lecturer in the Naval Academy, Varna. His research interests are in the theoretical and practical aspects of organization, planning and control of naval formations; organization of ship service and methods for training of tactical elements of the Navy; organization, planning and control of the MCMO of the PCO; characteristics of terrorism, anti- and counterterrorist actions; protection of shipping in emergencies. He is the author of 2 books and more than 30 articles and reports. Married with two children.

I&S Monitor

- Information Technology and Terrorism: The Impact of Emerging Commercial Capabilities
- Counterterrorism Related Internet Sources

INFORMATION TECHNOLOGY AND TERRORISM - THE IMPACT OF EMERGING COMMERCIAL CAPABILITIES

Goran JOHNSON

The fourth International Workshop for CITMO (Commercial Information Technology for Military Operations) 2005 was held in the lovely city of Plovdiv, Bulgaria from 15 to 17 June 2005.

The theme for CITMO 2005 was *Information Technology and Terrorism – The Impact of Emerging Commercial Capabilities*. Since the governments, military and commercial sectors are major players in the war on terrorism, it is essential that each sector understands how to make the best use of the new and emerging technologies while denying critical capabilities to terrorist organizations. It is obvious that cooperation among the military and commercial sectors and across the nations will be necessary to reach this understanding so that appropriate actions can be taken in the commercial marketplace to steer technology in ways that are most productive and supportive of peace, stability, and prosperity.

The issue for IT is how we fuse and distribute sensitive information in a multi-security network to support the right decision makers in a timely manner with trustworthy/ dependable information and protect the sources should that be necessary. These are real challenges for IT, made more complex by a continuously changing set of disparate partners working across the network, anyone of which could potentially be a hacker or terrorist themselves. We must also consider how we link disparate organizations and many interested, but not necessarily coalition/ allied nations/ groups together to achieve common goals in the "war on terrorism." This is the ultimate cyber ad hoc network because it is forever shifting depending on the whim of the terrorist—in other words it is not necessarily predictable ahead of time—there is not a single threat that a coalition or allied group can focus on.

Issues such as parties/ platforms quickly entering or leaving the network, multi-level security, and trust, all come to mind as issues that are both technical and policy re-

lated and must co-evolve in years to come so that we get the right technology and policy ultimately in place to achieve our common goal to reduce the threat of terrorism.

In order to have a meaningful discussion of the issues stated in the paragraphs above, we were fortunate to have had presentations from a varied group coming from government, industry and academia offering information, latest technology, practices and experience learned. Some of the articles in this volume give the reader a taste of what had been presented.

As we came away from CITMO 2005, we were not only grateful for the input of our host country, Bulgaria, but also impressed by the wide-range of input from our participants. The work for CITMO 2006 is well underway and the subject of Information Technology and Terrorism will continue to be the focus.

COUNTERTERRORISM RELATED INTERNET SOURCES

POLICY

Declaration on Combating Terrorism 7764/04 JAI 94

http://ue.eu.int/uedocs/cmsUpload/79635.pdf/

In the aftermath of the attacks on Madrid on 11 March 2004, the European Council of the European Union adopted a Declaration on Combating Terrorism at the EU Summit in Brussels on 25 March 2004, reinforcing its determination to prevent and fight terrorism. The European Council declared that "the Union and its Member States pledge to do everything within their power to combat all forms of terrorism in accordance with the fundamental principles of the Union, the provisions of the Charter of the United Nations and the obligations set out under United Nations Security Council Resolution 1373 (2001)."

The Declaration sets out overarching objectives designed to improve co-operation between Member States and their police/security forces and to assist the victims of terrorism.

- To deepen the international consensus and enhance international efforts to combat terrorism;
- To reduce the access of terrorists to financial and economic resources;
- To maximize the capacity within EU bodies and member States to detect, investigate and prosecute terrorists and to prevent terrorist attacks;
- To protect the security of international transport and ensure effective systems of border control;
- To enhance the capability of the European Union and of member States to deal with the consequences of a terrorist attack;
- To address the factors which contribute to support for, and recruitment into, terrorism;

- To target actions under EU external relations towards priority Third Countries where counter-terrorist capacity or commitment to combating terrorism needs to be enhanced.

European Commission Action Paper, dated 18 March 2004 in response to the terrorist attacks on Madrid: Commission Action Plan

http://www.statewatch.org/news/2004/mar/Comm-Action-Plan.pdf

The European Council Declaration on Combating Terrorism, 25 March 2004, updated the Plan of Action bringing out the overarching objectives of the Declaration into strategically achievable tasks. The Plan of Action has 7 Objectives which are specific, measurable and achievable tasks for the European Union focusing on Member State and international co-operation, within Member States and the Union as a whole as well as externally with third country partners. The ability of Member States to cope with a terrorist attack and work in co-operation against the activities of terrorist within the Union is the aim of such co-operation.

The European Commission Communications

http://europa.eu.int/scadplus/leg/en/s22008.htm

In response to the European Council Declaration, the European Commission has published several Communications dealing with combating terrorism:

- Towards enhancing access to information by law enforcement agencies;
- Prevention, Preparedness and Response to terrorist attacks;
- Prevention and the Fight against Terrorist Financing through Measures to Improve the Exchange of Information, to Strengthen Transparency and Enhance the Traceability of Financial Transactions;
- Preparedness and the Consequence Management in the Fight against Terrorism;
- Critical Infrastructure Protection in the Fight against Terrorism, etc.

The main elements of the Communications are:

- INFORMATION EXCHANGE: improving the accessibility of Member State databases within the Union and exchange of information.
- ARGUS: overreaching crisis alert system to co-ordinate all of the crisis management programs of the Commission.
- LEN: the creation of a Legal Enforcement Network to facilitate greater exchange of information between the police forces of Member States.

- EPCIP: the creation of a European Programme for Critical Infrastructure Protection consolidating and bringing together the Commission capability to advise and assist in critical infrastructure protection measures.
- TRANSPARENCY/TRACEABILITY/EXCHANGE: to tackle the financing of terrorism the Commission wants greater co-operation and exchange of information to facilitate the tracing of terrorist funds.

NATO's Role in Confronting International Terrorism

http://www.acus.org/docs/0406-NATO_Role_Confronting_International_Terrorism.pdf

A Policy Paper by Richard A. Clarke, Barry R. McCaffrey, and C. Richard Nelson, (Washington, D.C.: The Atlantic Council of the United States, June 2004).

The report is based upon the insights of an expert working group convened by the Atlantic Council. A central element of the project design was for members of the working group to make visits to different European capitals in order to gain as thorough an understanding as possible of the variety of views in European countries on the nature of the terrorist threat, on its likely future evolution and on the possible roles for NATO in the Western response.

Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan

http://www.dhs.gov/interweb/assetlibrary/DHS_StratPlan_FINAL_spread.pdf

The Strategic Plan of the Department of Homeland Security (DHS) identifies seven goals: Awareness, Prevention, Protection, Response, Recovery, Service, and Organizational Excellence. The first five goals relate directly to the Department's role in achieving the National Strategic Objectives for homeland security. The Service goal addresses DHS missions that are executed in tandem with the Department's homeland security mission responsibilities, and the Organizational Excellence goal speaks to DHS's commitment to be an effective steward of government resources.

National Counter-Terrorism Plan for Australia (June 2003, second edition September 2005)

http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/Page/Publications

The Australian National Counter-Terrorism Plan, prepared by the Australian National Counter-Terrorism Committee, outlines responsibilities, authorities and the mechanisms to prevent or manage acts of terrorism and their consequences within Australia.

A National Counter-Terrorism Handbook, which sets out in detail relevant procedures and protocols, supports the National Counter-Terrorism Plan.

Protecting Australia against Terrorism

http://www.pmc.gov.au/publications/protecting_australia/

On 23 June 2004, the Australian Prime Minister officially launched the Australian Government's comprehensive overview of Australia's national counter-terrorism policy and arrangements. This publication, *Protecting Australia against Terrorism*, explains the government's strategies for confronting the threat of terrorism in a complex and challenging security environment. It (1) describes the features of the new security environment; (2) outlines Australia's national framework and arrangements for countering terrorism, and (3) explains the steps the Australian Government has taken to protect Australians and Australia's interests against the threat of terrorism.

Homeland Security: Observations on the National Strategies Related to Terrorism (September 2004)

http://www.gao.gov/new.items/d041075t.pdf

This testimony of Norman J. Rabkin, Managing Director, Homeland Security and Justice Issues of the United States Government Accountability Office, before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, discusses the following issues: (1) To what extent are elements of the *Homeland Security and Combating Terrorism* strategies aligned with recommendations issued by the 9/11 Commission; (2) What Key departments have responsibilities for implementing the *Homeland Security* strategy, and what actions have they taken to implement the strategy; and (3) What challenges are faced by key departments in assessing their progress towards achieving homeland security objectives.

Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism (February 2004)

http://www.gao.gov/new.items/d04408t.pdf

This statement of Randall A. Yim, Managing Director, Homeland Security and Justice Issues of the United States General Accounting Office (GAO), discusses the seven national strategies related to combating terrorism and homeland security published by the Bush Administration following the attacks of September 11, 2001. This statement attempts to identify and define the characteristics of an effective strategy

and evaluate whether the national strategies address those characteristics. The characteristics GAO identified are: (1) purpose, scope, and methodology; (2) problem definition and risk assessment; (3) goals, subordinate objectives, activities, and performance measures; (4) resources, investments, and risk management; (5) organizational roles, responsibilities, and coordination; and (6) integration and implementation.

Federal Bureau of Investigation Strategic Plan 2004-2009

http://www.fbi.gov/publications/strategicplan/stategicplantext.htm

This Strategic Plan presents the FBI's forecast on terrorism and their strategic goal to protect the United States from terrorist attack, strengthening the three inextricably linked core functions – intelligence, investigations, and partnerships.

The Counterterror Coalitions: Cooperation with Europe, NATO, and the European Union

http://www.rand.org/pubs/monograph_reports/2005/MR1746.pdf

A report by Nora Bensahel, MR 1746 (Santa Monica, CA: RAND Corporation, 2003).

Shortly after the September 11 attacks, Air Force Chief of Staff General John Jumper asked RAND to conduct a study entitled "Thinking Strategically about Combating Terrorism." This year-long project was divided into four research tasks, each tackling different but complementary aspects of the counterterrorism problem:

- Threat assessment: identifying the character and boundaries of the threat;
- The international dimension: assessing the impact of coalition and other international actors on U.S. options;
- Strategy: designing an overarching counterterrorism strategy;
- Implications for the Air Force: identifying promising applications of air and space power.

The research for this report was conducted as part of the second task. The report is also part of a series on international counterterrorism cooperation. It examines European responses to the September 11 attacks and the subsequent war in Afghanistan, and assesses the types of cooperation that the United States will need from Europe to achieve its counterterrorism objectives. It also assesses the ways in which NATO and the European Union are reforming their agendas to address the threat of terrorism and the areas of mutual cooperation that will most benefit the United States.

Al Qaeda, Trends in Terrorism and Future Potentialities: An Assessment

http://www.rand.org/pubs/papers/P8078/P8078.pdf

A paper by Bruce Hoffman, (Washington, D.C.: The RAND Corporation, 2003).

This paper assesses current trends in terrorism and future potentialities. It examines first the presumed state of Al Qaeda today with particular reference to its likely agenda in a post-Iraq war world. It then more broadly focuses on some key current terrorism trends in order to understand better both how terrorism is changing and what the implications of these changes are in terms of possible future attacks and patterns. The discussion is organized along three key questions: What is the state of Al Qaeda today and what effects have 18 months of unremitting war had on it?; What do broader current trends in terrorism today tell us about future potentialities?; and How should we be thinking about terrorism today and tomorrow?

Homeland Security Policy

http://www.psk.org.vt.edu/psk2/papa6664-2006/background_readings/Selected_HS_webpages_and_reports--6664.htm

A comprehensive list of selected Homeland Security web pages and reports related to homeland security policy, updated on 10 February 2006.

SCIENTIFIC SUPPORT, TECHNOLOGIES

The Role of Systems Engineering in Combating Terrorism

http://www.incose.org/ProductsPubs/pdf/techdata/SEInit-TC/RoleOfSEInCombattingTerrorism_2003-0411.pdf

This is an article by William F. Mackey, Harry Crisp, David Cropley, James Long, Stephen Mayian, and Shabaz Raza, published in the INCOSE (International Council on Systems Engineering) 13th Annual International Symposium Proceedings, Washington, DC, July 2003.

The members of INCOSE Anti-Terrorism International Working Group (ATIWG) are applying the multidisciplinary approach of systems engineering to understanding all facets of terrorism. The ATIWG convened a special panel “The Role of Systems Engineering in Combating Terrorism” at INCOSE 2002 symposium in Las Vegas, NV. Rather than lose the information conveyed during that session, many of the pan-

elists agreed to join their efforts to coauthor this paper and document much of what was said.

This paper's thesis is that the multidisciplinary approach of systems engineering is useful in evaluating terrorist threats, identifying potential target vulnerabilities, and reducing or eradicating international terrorism. The systems engineering approach is most amenable to such evaluations because of its use of multiple disciplines to examine all facets of the problem space.

The reader may also consult the following paper: James Long and William F. Mackey, "Systems Engineering Modeling Useful in Combating Terrorism," in INCOSE 13th Annual International Symposium Proceedings, Washington, DC, July 2003.

Priorities in the Defense against Terrorism (DAT) Program of the NATO Conference of National Armaments Directors (CNAD)

http://www.nato.int/issues/dat/index.html

NATO's Defence against Terrorism (DAT) Program of Work is focused on several key areas where it is believed technology can help.

Individual NATO countries or Conference of National Armaments Directors (CNAD) groups are leading the various projects with support and contributions from other member countries.

The main areas in the program are:

1. Reducing the vulnerability of large-body civilian and military aircraft to man-portable air defence missiles (MANPADs).
2. Protecting harbors and ships from explosive-packed speedboats and underwater divers using sensor-nets, electro-optical detectors, rapid reaction capabilities and unmanned underwater vehicles.
3. Reducing the vulnerability of helicopters to rocket-propelled grenades (RPG).
4. Countering improvised explosive devices (IEDs), such as car and roadside bombs, through their detection and destruction or neutralization.
5. Precision airdrop technology for special operations forces and their equipment.
6. Detection, protection and defeat of chemical, biological, radiological, and nuclear (CBRN) weapons.

7. Intelligence, surveillance, reconnaissance and target acquisition of terrorists, with the goal of developing improved tools for early warning identification of terrorists and their activities.
8. Technologies to defend against mortar attacks.
9. Explosive ordnance disposal (EOD), with the objective of preventing existing stockpiles of munitions from falling into the hands of terrorists and of improving NATO's technological and operational capabilities to dispose of such stockpiles.
10. Protection of Critical Infrastructure.

Homeland Security Advisory System

http://www.nationalterroralert.com/overview.htm

This is the website of a Homeland Security advisory system and resources. It provides Homeland security guides for preparing against terror attacks and a free 300-pages homeland security manual.

NATO Science and Technology Topics on "Defense against Terrorism"

http://www.nato.int/science/how_to_apply/topic_supported.htm

The priority research topics in the area of Defense against Terrorism are concerned with the science involved in, for example, progress in detecting chemical, biological or radiological nuclear weapons or agents, or with physical protection against such weapons. Improved decontamination possibilities are also needed, as well as improved methods of safe destruction for these types of weapons or agents. Progress in medical responses to counteract such weapons will also be sought, for example chemical and vaccine technologies. Measures to protect against eco-terrorism and computer terrorism are two more areas earmarked for concentrated study.

Making the Nation Safer: The Role of Science and Technology in Countering Terrorism (2002)

http://www.nap.edu/books/0309084814/html/

This book by the Committee on Science and Technology for Countering Terrorism of the U.S. National Research Council of the National Academies, published by the National Academies Press describes the various ways in which science and engineering can contribute to countering terrorism. It identifies key actions that can be undertaken, based on knowledge and technologies in hand, and, equally importantly de-

scribes key opportunities for reducing current and future risks even further through longer-term research and development activities.

Understanding Why – Dissecting Radical Islamist Terrorism with Agent-Based Simulation

http://www.fas.org/sgp/othergov/doe/lanl/pubs/las28/why.pdf

This is an article written by Edward P. MacKerrow in Los Alamos Science, Number 28, November 2003.

The article discusses how Los Alamos scientists use computer simulations to gain insight into the nature of Islamist terrorist organizations. Based on techniques from the field of computational economics and sociology, they develop agent-based models that simulate social networks and the spread of social grievances within those networks.

The computer-generated "agents" are humanlike, with personal attributes and allegiances that statistically match the demographics of a specified region and, like people, interact with one another and respond to societal pressures. The agents can be exposed to a variety of determinants—new government policies, different media exposure, economic pressures, and others—and hundreds of new scenarios could be quickly generated. The goal, according to MacKerrow is to develop "a detailed understanding of the sociodynamics of militant Islamic terrorism."

Missile Defense Technologies: Tools to Counter Terrorism (2002)

http://www.mdatechnology.net/pdf/terror.pdf

This report of the Missile Defense Agency, U.S. Department of Defense, covers technologies that can be applied towards three areas of the counter-terrorism effort: chemical and biological countermeasures, surveillance and information collection, and cyber warfare.

More reports on the application of missile defense technologies can be found at: http://www.mdatechnology.net/specialreports.asp.

Understanding Terror Networks

http://www.upenn.edu/pennpress/book/14036.html

A book by Marc Sageman, published in April 2004 by the University of Pennsylvania Press.

Based on intensive study of biographical data on 172 participants in the jihad, this book provides social explanation of the global wave of activity. Sageman traces its roots in Egypt, gestation in Afghanistan during the Soviet-Afghan war, exile in the Sudan, and growth of branches worldwide, including detailed accounts of life within the Hamburg and Montreal cells that planned attacks on the United States.

The author refutes the traditional explanation that factors such as poverty, trauma, madness, or ignorance drive people to terrorism. Instead he highlights the crucial role of social networks in the transformation of socially isolated individuals into fanatical mujahideen. This book combines theories with empirical data to provide valuable insights.

An article with the same name by Marc Sageman that discusses social-network analysis of terror networks can be found at <http://www.mipt.org/Understanding-Terror-Networks-Sageman.asp>.

Framing the Terrorism Problem from an Engineering Point of View (September 2005)

http://www.sandia.gov/ACG/documents/papers/naf_workshop1.pdf

These are remarks by Gerold Yonas, Vice President & Principal Scientist at Sandia National Laboratories, from *Terrorism, Security, and America's Purpose: Towards a more Comprehensive Strategy*, an U.S. National Policy Forum Marking the Fourth Anniversary of 9/11.s

Gerold Yonas discusses terrorism by describing it in the framework of the theory of complex adaptive systems. Assuming this systems engineers' point of view, the author views the problem as consisting of three major components: (1) the threat, (2) the vulnerabilities of the targets of terrorism, and (3) the consequences of any action; the solution could be divided into three parts: (1) preparation, (2) protection, and (3) response. Gerold Yonas then discusses "some high-risk problems and high payoff developments that would support a system solution."

Project Responder: National Technology Plan for Emergency Response to Catastrophic Terrorism (April 2004)

http://www.mipt.org/pdf/2004-MIPT-Terrorism-Annual.pdf

Since April 2001, the U.S. National Memorial Institute for the Prevention of Terrorism (MIPT) has funded Project Responder, an effort by Hicks & Associates, Inc. and the Terrorism Research Center, Inc., aimed at improving local, state and federal emergency responders' capabilities for mitigating the effects of chemical, biological,

radiological, nuclear or explosive/ incendiary (CBRNE) terrorism. As a result of this effort, the report is a technology roadmap for federal planners to fill gaps in emergency responder capability against CBRNE terrorism.

The Future of Anti-Terrorism Technologies (June 2005)

http://www.heritage.org/Research/HomelandDefense/hl885.cfm

This Lecture #885 was given by James Jay Carafano, Ph.D. of the Heritage Foundation on June 6, 2005.

The lecture's thesis is that meeting the test of terrorism will likely require a more proactive approach to technological innovation: betting on the future, formulating clear requirements, prioritizing needs, establishing cooperative means to foster the development of technologies, and building the human and financial capital programs necessary to transition and sustain them as effective anti-terrorism tools.

The author lists six technologies that he believes offer the greatest promise for providing significant advantages in combating terrorism and addresses as well the challenge to turning the potential of technology into concrete capabilities. These six future technologies are: (1) system integration technologies; (2) biometrics; (3) non-lethal weapons; (4) data mining and link analysis technologies; (5) nanotechnology; and (6) directed-energy weapons.

Fusing Intelligence with Law Enforcement Information: An Analytic Imperative (March 2005)

https://www.hsdl.org/homesec/docs/theses/05Mar_Thornlow.pdf

This Master's thesis by Christopher C. Thornlow, Naval Postgraduate School, Monterey, CA, Department of National Security Affairs, discusses the challenges faced by the United States Northern Command Intelligence Directorate (J2) counterterrorism analysts as they try to produce products that are "accurate, timely, and relevant," using all available information sources, including law enforcement information. Thus, fusing and analyzing foreign threat intelligence with domestic law enforcement information in a timely fashion will provide adequate indications and warning of terrorist attacks.

Principles of Prevention and the Development of the Prevention Triangle Model for the Evaluation of Terrorism Prevention (March 2005)

https://www.hsdl.org/homesec/docs/theses/05Mar_Longshore.pdf

This Master's thesis by David M. Longshore, Naval Postgraduate School, Monterey, CA, Department of National Security Affairs, proposes theoretical and practical development of the "Prevention Triangle," a graphical model designed to define a system for evaluating national, state, and local terrorism prevention mandates and programs. "Based upon objectives detailed in the National Strategy for Homeland Security, and derived through an analysis of selected prevention theories and programs—primarily those aimed at crime prevention—this study first seeks a theoretical basis for the prevention of terrorism in the form of four principles before deriving and defining representative evaluative criteria for designing and measuring the efficacy of prevention programs."

Distribution of Transnational Terrorism among Countries by Income Classes and Geography after 9/11 (January 2005)

http://www.usc.edu/dept/create/reports/Enders-Sandler_10-04.pdf

This article by Walter Enders and Todd Sandler from the Center for Risk and Economic Analysis of Terrorism Events at the University of Southern California applies an autoregressive intervention model for the period 1968-2003 with the objective to identify either income-based or geographical transference of transnational terrorist events in reaction to the rise of fundamentalist terrorism, the end to the Cold War, and 9/11. This time-series study investigates the changing pattern of transnational terrorism for all incidents and those involving U.S. people and property. Based on the empirical findings from this study, the authors draw policy recommendations regarding defensive counterterrorism measures.

Planning for Success: Constructing a First Responder Planning Methodology for Homeland Security (March 2005)

https://www.hsdl.org/homesec/docs/theses/05Mar_Jankowski.pdf

This Master's thesis by Thaddeus Jankowski, Naval Postgraduate School, Monterey, CA, Department of National Security Affairs, argues that the planning methodologies used today by most U.S. fire departments are excellent for traditional missions, but wholly inadequate for the threats posed by terrorism. The author argues that the fire service and others in the first responder community will be able to contribute to homeland security missions much more effectively, and efficiently, by switching to specially adapted versions of capabilities-based planning rather than using the traditional scenario-based planning approach. The thesis proposes a new integrated planning methodology that combines the planning strengths of scenario-based planning, threat-based planning, and capabilities-based planning. The new method identifies

capabilities that could be used to manage and mitigate the consequences of the different types of contingencies within the various response spectrums

OTHER PUBLICATIONS AND USEFUL SITES

NATO Review, Special Issue on Combating Terrorism (Autumn 2005)

http://www.nato.int/docu/review/2005/issue3/english/main.htm

This special issue of NATO Review features the following contributions:

- NATO's Response to Terrorism (Dagmar de Mora-Figueroa examines how NATO has responded to the terrorist threat since the 11 September terrorist attacks against the United States)
- NATO-Russia Cooperation to Counter Terrorism (Andrei Kelin describes how NATO and Russia are forging an increasingly effective partnership to combat the terrorist threat)
- Combating WMD Proliferation (Eric R. Terzuolo considers NATO's role in combating the proliferation of weapons of mass destruction)
- Combating Terrorism in the Mediterranean (Vice Admiral Roberto Cesaretti examines how NATO has been combating terrorism in the Mediterranean since October 2001)

The MIPT Terrorism Annual 2004

http://www.mipt.org/pdf/2004-MIPT-Terrorism-Annual.pdf

This report of the U.S. National Memorial Institute for the Prevention of Terrorism, with contributions from Audra K. Grant and William Rosenau, published in 2005 discusses recent trends in global terrorist activity, with an aim of identifying the world's most active terrorist groups, based on statistics from the RAND-MIPT Terrorism Incident Database.

U.S.-EU Cooperation against Terrorism (January 2006)

http://www.fas.org/man/crs/RS22030.pdf

This U.S. Congressional Research Service (CRS) report discusses the challenges the United States and European Union (EU) face "as they seek to promote closer cooperation in the police, judicial, and border control fields."

Counter-terrorism Conference Calendar

http://www.mipt.org/eventscalendar.asp

This is a directory of upcoming counter-terrorism-related conferences.

Courses and Training Events

http://www.mipt.org/trainingcourses.asp

This resource, compiled by MIPT, is a database of various courses and training events offered by different institutions across the United States.