CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM

COE-DAT
Newsletter

Volume 1 / Issue 4 / November 2007

Contents

3 **General Overview of the Terrorist Activities**
by Ömer YILMAZ
Inspector, TUR Police

7 **What are the Best Metrics of Success When Fighting Terrorists?**
by Engin KILIÇ
Captain (TUR N)

9 **Account of the ARW "Responses to Cyber Terrorism"**
by Osman AYTAÇ
Colonel (TUR A)

16 **Al-Qaeda's Religious Terrorism and The New Cold War**
by Çınar ÖZEN
Assoc.Prof. (ACAD)

19 **Religious Motivations for Terrorism**
by Julian CHARVAT
Major (GBR A)

25 **Terrorism and The Media**
by Alexandru A. TEODORESCU
Lt.Col. (ROU A)
Julian CHARVAT
Major (GBR A)

30 **COE-DAT Activities**

COE-DAT;

Your gate to get information.

Editorial

In the fourth issue of Newsletter, first of all, we provide you a review of the worldwide terrorist incidents took place between Sep.1 and Oct.15, 2007. In addition, we have three articles and two course reports.

In his essay, "*What are the Best Metrics of Success When Fighting Terrorists*", Captain (N) KILIÇ, argues some determinants which can be used for an effective the fight against terrorism.

Colonel AYTAÇ, points out the general concept of the essays presented in the advanced research workshop of "Responses to Cyber Terrorism" which was held on 04-05 October 2007.

Assoc. Prof. ÖZEN examines the ideology of al-Qaeda, its effects on international system and concludes that al-Qaeda's ideology is not capable of achieving its goals in his essay "Al-Qaeda's Religious Terrorism and the New Cold War".

Major CHARVAT, in his article "*Religious Motivations for Terrorism*", notes some motivations of different religions which are used for justification of terrorist aims; the effect of religions on terrorism and the way to deal with this threat.

LTC TEODORESCU and Major CHARVAT gives us some useful information about the topic "Terrorism and The Media". In this article, the subjects like "Terrorist Broadcasts and Messages in The Mass Media" and "The Internet as a Media for Terrorists" are presented.

The opinions and comments in the "*COE-DAT Newsletter*" represent
the personal views of the authors. They do not represent the official views of
Centre of Excellence Defence Against Terrorism nor NATO.
All the rights of the articles and pictures included in this book are reserved.

General Overview of the Terrorist Activities (01 September -15 October 2007)

Ömer YILMAZ
TUR Police, Inspector, Analyst

In this one and a half month period, comprising September and the first half of October 2007, several terrorist incidents have been reported from 31 different countries all around the world, according to the information available retrieved from both international and national news agencies. As a result of total 1241 attacks, 2491 people lost their lives and 3636 more sustained various injuries. The abductions of 199 others were the other security challenges in the relevant time period.

Iraq was, far and away, the most volatile country in the world as for the number of attacks conducted and the casualty levels that some 556 separate attacks claimed 1328 lives and 1918 injuries. Although can not be regarded as acceptable, these figures are one of the slightest ones in the year 2007. And the main reason for this decline was undoubtedly the prevention of conducting large-scaled suicide attacks or vehicle borne IED-strikes. However, in the single largest attack, which was a VBIED-strike, 32 people lost their lives and 28 others sustained injuries on September 26 in the capital Baghdad city. In addition to the capital city, Mosul and Kirkuk were the main troubled cities in Iraq.

In the second-most hit country, **Afghanistan**, the violence continued in the relevant period with some 155 attacks, killing 313 people and wounding 370 others. In the single largest attack which occurred in the capital Kabul city on September 29, thirty-one people lost their lives and seventeen more sustained several injuries when a suicide bomber, acting like a passenger, blew himself up in front of a Afghan National Army bus. The southern Helmand, eastern Paktia and north-eastern Kunar provinces were recorded as the most volatile locations in the country.

In **India**, the decrease in the number of attacks saw a third month after June 2007 and continued in the first half of October and some 125 attacks claimed 143 lives and 186 injuries in the relevant time. 15 more people were also abducted by the suspected militants in the country. Both the level of fatalities and the casualties were recorded as the one of the least ones in the year 2007. The twin bombings in north-eastern Assam state in the last day of the month were the most significant attacks of the month, which were purportedly carried out by the separatist United Liberation Front of Asom (ULFA). In these attacks total five people were killed and 52 more were wounded. However, the deadliest attack was carried out in Jammu and Kashmir on October 11. In this IED-strike, eleven people were killed and six more were wounded.

Having reached its peak in August 2007, the violence in **Pakistan** experienced a one-third decrease in September and a similar tendency was also observed in the first half of October. Despite this significant decrease, Pakistan became the second most-hit country in Asia. Besides, the casualties given in the terrorist attacks were also the highest of the continent. Indeed, some 116 separate attacks claimed 245 lives and 412 injuries in the relevant time period. The twin attacks which were carried out in Rawalpindi on September 4 were the most significant attacks took place in the country and claimed 30 lives, along with 70 injured.

Separately in **Asia**, the terror campaign of Liberation Tigers of Tamil Eelam in Sri Lanka claimed 88 lives and 117

COUNTRY	Event Count	KIA	WIA	AIA
Afghanistan	155	313	370	51
Algeria	4	52	168	0
Argentina	1	0	1	0
Bangladesh	3	1	2	2
Chad	1	20	0	0
Colombia	2	3	0	20
East Timor	1	0	0	0
Georgia	1	2	0	0
Greece	1	0	0	0
India	125	143	186	15
Iran	4	8	3	1
Iraq	556	1328	1918	63
Israel	4	1	57	0
Lebanon	2	7	92	0
Mexico	1	0	0	0
Myanmar	2	4	4	0
Nepal	27	26	45	3
Niger	1	0	0	6
Nigeria	1	1	0	2
Pakistan	116	245	412	35
Philippines	4	12	28	0
Maldives	1	0	12	0
Russia	6	15	12	0
Somalia	51	111	54	1
Spain	3	0	1	0
Sri Lanka	73	88	117	0
Sudan	4	23	18	0
Thailand	46	44	68	0
Turkey	43	40	64	0
USA	1	0	0	0
Yemen	1	4	4	0
Grand Total	**1241**	**2491**	**3636**	**199**

Table 1 *- Incidents throughout the World*

injuries in 73 attacks while the southern insurgency in Thailand resulted in the deaths of 44 people and wounded 68 more in 46 attacks. In addition, Nepal, Philippines, Bangladesh, East Timor, Myanmar and the Republic of Maldives were recorded as the other countries suffered from terrorist activities in the relevant period.

In the **Middle East**, the month was marked by the assassination of a law-maker in Lebanon in a vehicle borne IED-attack that killed five people and wounded 92 more. In addition, the **PKK/KONGRA-GEL-affiliated PJAK**'s activity in Iran, the indirect fire attacks of Palestinian militants at Israeli land and the armed attack in Yemen were the other security developments in the region.

Africa saw relatively calm days in the relevant period and from only six countries some terrorist attacks were reported. However, the worsening situation in Somalia had affected the information flow from the country and accordingly only 51 attacks could be noted during the month. Separately, Algeria was again hit hard by the al-Qaeda off-shot in the country with two suicide attacks and as many IED-strikes. Separately, four incidents were reported from Sudan and Chad, Niger and Nigeria were hit for once.

In the relevant time period **four European countries** were hit by several terrorist incidents. **Turkey** was far and away the most hit country by terrorism, shaped mainly by the terrorist **activities of the PKK/KONGRA-GEL terrorist organization**, in Europe while the clash between the Georgian security forces

EVENT TYPE	Event Count	KIA	WIA	AIA
Abduction	41	1	0	177
Armed Attack	457	1094	301	20
Arson	10	0	2	0
Assassination	50	54	117	0
Clash	163	344	313	1
Execution	2	4	0	0
Hijack	2	0	1	0
Hoax	2	0	0	0
Hostage Kill	17	24	0	1
IDF	79	63	380	0
IED	237	248	854	0
Infrastructure Attack	15	0	0	0
NA	2	3	0	0
Suicide Attack	59	356	731	0
VBIED	54	242	815	0
VOIED	51	58	122	0
Grand Total	**1241**	**2491**	**3636**	**199**

Table 2 *- Types of Terrorist Attacks Used*

and the Abkhazian fighters, three ineffective IED-strikes in Spain and six armed attacks in Russia's troubled regions were the other incidents took place in the month. A hoax was also reported from Greece's Athens on October 15.

Lastly, **Americas** saw a peaceful month in the relevant period. However, two incidents in Colombia resulted in three deaths and 20 abductions. Excluding Colombia, the sole attack resulted in casualties was reported from Argentina when a letter bomb was exploded in the hands of a manager of a foreign firm. The IED-strikes targeting Mexico's gas ducts raised the concerns on the energy safety after the July attacks and the bomb hoax in USA was the other incident recorded on the continent.

The terrorists used fifteen different tactics in the relevant period around the world and the **close quarter armed attacks** were again the most repeated tactic with 457 occasions, killing 1094 people and wounding 301 more. The total number of those found dead in this period showed a significant decrease and was noted as 546. Separately, in 163 clashes, mainly the security forces gave 344 loses and 313 injuries.

The level of **suicide attacks** also didn't change much in this period and 59 such attacks claimed 356 lives and 731 injuries in Afghanistan, Algeria, Iraq, Pakistan and Somalia. The largest suicide attack was the one in Algeria which killed at least 19 people and wounded 107 others on September 6 in the Batna region.

As another deadly attack type, the vehicle borne improvised explosive device (**VBIED**) attacks claimed 242 lives and injured 815 more in 54 incidents. Iraq, Pakistan, India, Spain, Sri Lanka and Turkey were the

EVENT TYPE	COUNTRY	Count of EVENT TYPE	KIA	WIA
IED	Afghanistan	29	64	77
	Algeria	2	3	14
	East Timor	1	0	0
	India	13	26	112
	Iraq	129	126	436
	Mexico	1	0	0
	Myanmar	1	3	4
	Nepal	5	3	27
	Pakistan	22	10	61
	Philippines	1	2	26
	Maldives	1	0	12
	Somalia	6	5	16
	Spain	2	0	0
	Sri Lanka	3	2	9
	Thailand	11	2	48
	Turkey	10	2	12
IED Total		*237*	*248*	*854*
Suicide Attack	Afghanistan	21	110	151
	Algeria	2	49	154
	Iraq	27	106	297
	Pakistan	8	89	129
	Somalia	1	2	0
Suicide Attack Total		*59*	*356*	*731*
VBIED	India	1	0	7
	Iraq	49	240	779
	Pakistan	1	0	24
	Spain	1	0	1
	Sri Lanka	1	1	0
	Turkey	1	1	4
VBIED Total		*54*	*242*	*815*
VOIED	Afghanistan	9	11	18
	Argentina	1	0	1
	India	3	2	1
	Pakistan	7	20	35
	Somalia	2	4	0
	Sri Lanka	11	14	41
	Thailand	1	1	0
	Turkey	17	6	26
VOIED Total		*51*	*58*	*122*
Grand Total		401	904	2522

Table 3 *- Types of IED-Strikes and Casulties per Country*

countries hit by such attacks. The VBIED attack of September 26 in Baghdad was the deadliest one as 32 people lost their lives and 28 others sustained injuries in the attack. A similar attack which hit Mosul on September 10 also killed ten people and wounded at least 78 more.

The landmine attacks, as a terrorist tactic, hit Turkey most in the relevant period and six people were reportedly killed and 26 others were wounded in such 17 PKK/KONGRA-GEL attacks. Such devices were also used in Afghanistan, Sri Lanka, Pakistan, India, Somalia and Thailand. The other details of IED-usage in terrorist attacks can be found in Table 3.

What are the Best Metrics of Success When Fighting Terrorists?

Engin KILIÇ
Capt (TUR N)
Chief, Education and Training Department, COE-DAT

1. Introduction

One must clearly define terrorism and the best metrics of success when fighting terrorists in order to properly discuss the answer to the question.

Just as strategies to counter terrorism vary with every situation, the definition of terrorism varies as a result of perspective, political influences, opinions of instruments and techniques used by belligerents, rationality of the belligerents, and a host of other reasons.

Nevertheless, for the purposes of this analysis terrorism is defined as an act and a tactic used by a small set of extremists to fight against an overwhelmingly powerful opponent while surrounded by a large population who mostly just want peace and quiet. This definition, although simple, reflects the common theme of terrorist activity while avoiding details that may muddle its meaning. Ironically, throughout history, the details of counterterrorism strategy were often a mirror image of the activities of terrorists.

Today, there is no specific definition of the best metrics of success when fighting terrorists. We lack metrics to know if we are winning or losing the war on terror. Are we capturing, killing or deterring and dissuading more terrorists every day than the terrorists are recruiting, training and deploying against us?

What are metrics? "Metrics" is a fancy word for "measurements" that matter to management. A metric can be something like the number of customers who enter a retail store on a given day. In the terrorism context, it can be some other indicator, such as the number of terrorists in custody.

2. Thesis:

The world today is faced with the dilemma of formulating the best metrics of success when fighting terrorists. However, these metrics will differ from case to case. The answer to the question of what are the best metrics of success when fighting terrorists lies in an unsatisfactory history. That frustrating history has shown us only one historical absolute when analyzing terrorism–the most effective response to terrorists is unique to the case at hand. On the other hand, history has taught us that there are common aspects, which warrant analysis, to these metrics of success.

If you choose the wrong metrics, your execution will invariably orient on those metrics and produce unintended results.

Here are certain metrics which have become accepted measures of success or failure by default, including:

- Capturing or killing the leadership of the terrorist organization;

- Disconnecting the leader of the terrorist organization and his supporters from power;

- The number of battle and non-battle casualties;

-The number of high-value enemy captured;

- The number of terrorists events, per week, in the country;

- The total amount spent time and resources on fighting terrorists;

-The level of the community's trust in the local authorities in maintaining law and order and working for the common good;

- In my view, the most important metric that matters in the country's war on terror is the number terrorist attacks on the country's persons or interests at home and abroad.

3. Argument:

In addition to developing different metrics for different time frames, metrics should also be both quantitative and qualitative in character. This is not to dismiss the importance of metrics such as the rate of attacks around the world, the number of terrorist ring leaders killed or captured and the value of assets frozen. Rather, the point is that we should also seek to define other measures that provide another angle of insight into our progress.

A combination of tactical, strategic, quantitative and qualitative metrics is probably the best way to measure progress. Devising and developing these various metrics is worth some effort.

The closer to zero we can get that measurement, the closer we get to victory. Every other measurement of success and every other strategy ought to be included in this aggregate metric. At best, one can make an attenuated argument that winning the hearts and minds of people will help to reduce the recruitment pool for terrorists, but that is almost unquantifiable.

There are surely many other metrics of success when fighting terrorists, such as:

- *Terrorists in the country custody,*

- *Money frozen through anti-terrorism financial investigations,*

- *Number of suspected terrorists denied entry visas, etc.*

In *the end; the only thing that matters is that we never see another attack on the country again.* That's how we ought to measure success.

It's tempting to think that the best metrics of success when fighting terrorists are killing all the terrorists. In the real world, this naive plan doesn't work. A serious attempt to find and kill all the terrorists cause innocent casulties amnog the population and some of them and their relatives will become new terrorists, creating more terrorists than were defeated. The harder the authorities pursue this strategy, the more effectively they recruit new terrorists. One of the best metrics of success is the trust and cooperation of the population of the country.

Apart from these metrics of success, there are surely many other good metrics of success to be identified, improved, evaluated, and applied, such as:

- *Gaining the trust and Cooperation of the population in the country*

- *Destroying terrorist networks and the infrastructure of the terrorist movement;*

- *Cutting-off the terrorist's financial lifeline;*

- *Using all elements of national power to deny terrorist recruiting,*

Time usually favors the terrorists. Governments are not able use force as effectively as in a conventional war. The terrorists usually want a protracted war. They have much lower costs in military equipment and supplies than a government must expend in defeatin an uprising.

As the costs mount, governments must change their strategy or be willing to stop fighting once the value of the objective exceeds the costs of fighting. The only way of effectively fighting terrorists is to provide the security and welfare of the local population and to provide them the chance to aid the government in fighting and eliminating the enemy piece by piece.

4. Conclusion:

a. Asking the question of what the best metrics of success when fighting terrorists will often create frustration, variance and disparity. Today, there is no specific definition of the best metrics of success when fighting terrorists. We lack metrics to know if we are winning or losing the war on terror.

b. One can argue that capturing, killing or deterring and dissuading more terrorists than terrorists are being recruited, trained and deployed against us is the metric of success.

c. The most important metric that matters in the country's war on terror is the the number of terrorist attacks on the country's persons or interests at home and abroad, in other words, we should never see another attack on the country again.

d. Consequently some good examples of measures for success could be the absence of attacks against government institutions, a significant decline in the appeal of the movement, sustained public support for counterterrorism measures, assistance from unlikely allies and a reduction in the networked quality of the movement.

e. There is no magic short cut to victory in countering the terrorism. The key to success is to properly evaluate their capability, the value of the objective for them and to properly identify the nature of the war. In addition to that, not to allow them to create a climate from which they can benefit. Since terrorism is a long-term endeavor, counter-terrorism must be similarly long-term in focus and thus the indications of possible success may not be immediately apparent.

f. Because terrorism seems to be a largely decentralized organization lacking a suitably identifiable target to attack by conventional military means, a subtle use of soft power such as diplomacy and persuasion should not be underestimated.

Account of the ARW "Responses to Cyber Terrorism" (04-05 October 2007)

Osman AYTAÇ
Col (TUR A)
Course Director, COE-DAT

Who's Afraid of Computer Code?

In the first week of October COE–DAT organized an Advanced Research Workshop (ARW) on the topic "Responses to Cyber Terrorism". The venue was the Merkez Ordu Evi (Central Officers' Club) in Ankara.

One issue touched on repeatedly by the speakers was the difficulty of arriving at a definition of this kind of terrorism. A NATO Office of Security document cautiously defines it as "a cyber attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal."(1)

But the cyber world is surely remote from what we recognize as terrorism: the bloody attacks and ethnic conflicts, or, more precisely, the politically-motivated "intention to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government …" (UN report, *Freedom from Fear*, 2005).

It is hard to think of one instance when computer code has physically harmed anyone. Yet a number of our speakers, in particular Prof. Goodman and Lt. Paul Everard, showed that we should be preparing for just such events, potentially on a huge scale. Here we are talking about attacks on critical infrastructure, in particular on SCADA (Supervisory Control and Data Acquisition) systems which control physical processes in places like chemical factories.

Focus on Solutions

At the planning stage of the ARW it was agreed that the workshop would bring together people from a range of disciplines, from information technology researchers and lawyers, to terrorism and security experts. The title "Responses to Cyber Terrorism" was chosen to put the onus on the discussion of practical solutions, and in some respects the meetings of the Working Groups were as important for achieving the goals of the ARW as the plenary sessions. In their presentations, the speakers all gave time to the issue of 'responding' to terrorism in cyberspace. In this summary of the two days, we also want to highlight the recommendations they made.

Freedom and Its Abuse

The first thing to emphasize is the internet's current vulnerability to attack. Its anonymous and open nature makes it very difficult to control, as is clear from the abundance of cyber crime, and (no small problem this) the tide of 'spam'. The internet's borderless interconnectivity means that 'malware' (malicious software) can be loaded from anywhere, and targeted at anywhere, in the world.

It is interesting to think that the internet need not have been so insecure. During its development there was such an enthusiasm for the free flow of information and user-driven design that the issue of security was deliberately neglected.

In the introductory first paper of the ARW, "The History of the Internet", Claire Cridland notes that the system was developed in the U.S. for military purposes. With ARPANET the

(1) Cited from Lt. Paul Everard's presentation

Defense Advanced Research Projects Agency (DARPA) created a network for sending packets of information with no central hub, so that communications could be more resilient during a devastating war. The idea of security was, therefore, part of the original idea of the internet.

However, an entirely different ethos took over after the Department of Defense relinquished the project to the burgeoning computer and software companies in the 1990s. The architects of the worldwide network saw it, and wrote of it, in terms of an expression of the centuries-old struggle for freedom of thought. Claire Cridland's description of the internet also evokes this theme: "New media in the early 21st century is a participatory, user-driven information environment, far from the linear platform of the mass media that delivered information through a 'gatekeeper' to a passive mass audience.
These outlets … were capital intensive and … somewhat privileged. In contrast, new media, driven by technological change in telecommunications, has undermined this sphere of knowledge ownership … However, we've been here before. 'Counter-culture' always used 'grassroots media' (folk songs, posters, leaflets, public meetings) rather than the more traditional mass media of radio and television to message audiences."

Contrast this 'triumph of the common people', then, with the more pessimistic comments on the freedoms the internet offers by Prof. Seymour Goodman in the third paper of the ARW, "Critical Information Infrastructure Protection". For example, at one point in his presentation he mentioned his friend Steve (Lukasik), who was involved from the outset with ARPANET. Steve, said Prof. Goodman, was the one person in ARPA who was concerned that security issues were being ignored in the architecture of the internet. At the time he yielded to his colleagues' enthusiasm for open access, but "he regretted that later, and has dedicated the latter part of his career to putting it right".

Prof. Goodman is a leading expert in the field of cyber defence. He is the chairperson of the Committee on Improving Cyber Security Research at the National Research Council, advising the U.S. Congress. Much of what the professor had to say, and this was reflected also in the Working Groups of the ARW, was a matter of pointing out the vulnerabilities in the globalized net, and the need for CIIP (Critical Information Infrastructure Protection) in view of the dangers of cyber terrorism. His chapter in this book also contains a wide range of recommendations for national and international action.

It is clear that the "current technology asymmetrically favours the attacker, and provides them with great non-linear leverage. The attackers can put their innovations into practice more quickly and effectively than the defenders." However, when much of the network is outsourced, or owned by companies in a variety of countries, defence is left to the end user. As Seymour Goodman writes, "most of the 200+ connected countries have little or no national cyber security capabilities." The users are often unaware of the seriousness of the risk. Frequently networks controlling important infrastructure are not 'air-gapped' (separated) carefully enough from the worldwide internet. If one employee's computer is not air-gapped, perhaps due to negligence, this is enough to create the route for an attacker to gain entry to the whole system.

There is a very real danger of the internet becoming a terrorist weapon, not just a terrorist tool. Even 'internet stalking', involving threatening e-mails being sent to a number of personal addresses, could be enough to achieve one of the terrorist's aims: to disseminate fear.

A List of Recommendations

In his presentation Professor Goodman gave a broad overview of the kind of recommendations his Cyber Security committee are considering. He began with general measures, which would be equally relevant to protection against accidents, disasters, crime, or forms of conflict apart from terrorism. Emergency response systems, including ones with an international dimension, must be in place; SCADA systems must be made more secure, with security as "a factor to be considered over the entire life cycle of any system that is part of the CII"; and countries "must build cadres of capable defenders" including national-level CSIRTs (Computer Security Incident Response Teams). On the issue of legal measures against cyber terrorism, Seymour Goodman mentioned the need for international conventions, as well as effective national laws. The conventions would relate to three areas: crime and punishment, infrastructure protection, and arms control. In each case he gave examples already in place which could guide developments in combating cyber terrorism. He saw agreements on civil aviation as the best model for similar work on CIIP. It would be difficult to gain acceptance for a CIIP convention, especially as every country would have to sign up, otherwise measures protecting the network could simply be by-passed. Such a convention could be under the umbrella of the UN, and it would involve an organization to build and certify national capabilities.

We were reminded that one hundred years ago there were no civil aviation conventions, but new technology was followed by effective international legislation and control. The same could be done to protect cyberspace.

Analysis of Cyber Attacks and Terrorist Contents

Phillip Brunst's paper, "Use of the Internet by Terrorists", is a highly analytical overview of the subject. This kind of paper would provide a good basis for considering an appropriate legislative approach. The overview covers both of the distinct aspects which emerged at the ARW: cyber terrorism proper, and the issue of terrorist use of the internet for communication, researching targets, etc..

After discussing the advantages of cyber attacks for the terrorist (anonymity, low cost, etc.), types of cyber attack are analyzed. In general, attacks on IT systems may take the following three forms: (1) Hacking attacks on individual systems, (2) Denial of Service (DoS) attacks, usually by bombarding a computer with messages so that it cannot process anything else, and (3) 'hybrid attacks' which combine one or both of the above with a conventional terrorist attack like a bombing.

(1) Hacking can be further analyzed into three types. The hacker can shut down a computer, although here the administrator can usually recognize the problem and restore the system rapidly. There are also so-called 'defacements', which alter the information on the victim computer. Typically these are easily recognized, especially if a hacker places a notice saying "you have been hacked by …". Potentially more disruptive are defacements which subtly change figures or other information. Thirdly, there is the possibility of introducing 'Trojan horse' programmes. These are silent operations, and aim to pass undetected by virus scanners. They gather data from the target computer (typically bank details in cyber crime) and relay it to the hacker.

(2) Distributed Denial of Service (DDoS) attacks are an effective way of putting computers out of action for a period of time. DoS attacks bombard a computer with vast numbers of messages, occupying all its processing capability. 'Distributed' attacks make use of worldwide networks of computers (so-called 'bot-nets', from their use of 'robot' software) infected with a virus which

allows them to be 'zombies' controlled by a 'bot-master'. These viruses have become very common. Terrorists would not have to control such systems. The services of a bot-net, typically used for mass mailings, can be hired for prices ranging between 150–400 US dollars per day.

(3) Hybrid attacks combine one or both of the above with a conventional terrorist attack. For example, a terrorist group might combine a bombing with a DoS attack to hamper the work of the emergency services.

Terrorists might target the physical hardware of IT communications, like the 'bundles' of cables, or the so-called 'peering points'.
All the above types of attack would harm IT data and lead to economic losses. A more fatal kind of cyber attack is now discussed in security circles, namely attacks on the newly-developed SCADA systems, which usually run on well-known operating systems like Windows. Many companies now use SCADA systems to monitor and control production or supply processes. When one considers that these include dams, chemical factories, airports, and food companies, it is clear that, if such a system is hacked, there is a considerable danger of the kind of loss of life associated with 'conventional' forms of terrorism.

Phillip Brunst's paper recommends measures to encourage companies to invest more in security. Secondly, referring to Article 35 of the CoE Convention on Cyber Crime, he sees a need for the establishment of designated communication paths within countries and between countries to fight digital attacks. On the issue of the terrorist presence on the internet, he sees efforts to block terrorist communications as bound to fail. These communications should be monitored for intelligence (see the presentations by Prof. Gabriel Weimann and Yael Shahar mentioned below).

Examples of Cyber Attacks

Lt. Paul Everard attended the workshop to represent the NATO Computer Incident Response Capability at the alliance's European Headquarters in Belgium. His presentation, "NATO and Cyber Terrorism", was an introduction to cyber terrorism and the defensive measures NATO is taking. Lt. Everard began by giving numerous illustrations of cyber attacks to show what directions cyber terrorism might take. There was the dramatic hacking of a SCADA system controlling sewage in Queensland, Australia: "Symantec research highlighted an Australian case where a disgruntled ex-employee, Vitek Boden, hacked into a computerized waste management system in Maroochy Shire and caused millions of litres of raw sewage to spill into local parks, rivers, and even the grounds of a Hyatt Regency hotel in March 2000."

If terrorists could replicate the destructive effects of the 'Slammer Worm' of January 2003, they would score a great success in their terms. This computer worm spread across the world in a matter of minutes, and the resultant disruption of banking, airline, infrastructure and emergency services had a high economic cost. Lt. Everard notes that "the safety monitoring system at a nuclear power plant was disabled for a combined period of eleven hours."

There have been various attacks on NATO, including attacks from Chinese hackers after NATO bombed the Chinese embassy in Belgrade (1999), and a distributed attack on the NATO mail server on 09–10 August 2006, when "the attack was stopped by re-configuring the mail server to respond correctly to the attempted e-mail relay traffic."

NATO's Cyber Defences

Paul Everard noted that NATO has long been aware of its vulnerability to cyber attacks. It generally uses 'off the shelf' software, the vulnerabilities

of which are well known to potential hackers. Also, "although NATO's internal networks are supposedly separated from the internet, documents, messages and other data are being uploaded onto the internal network constantly."

With the approval of the North Atlantic Council, the NATO Computer Incident Response Capability was added to InfoSec after 9/11. At present there is an Intrusion Detection Systems project which will be at full operating capacity in 2008. The Prague Summit of 21 November 2002 was attended by the leaders of NATO countries, who signed a commitment to "strengthen our capabilities to defend against cyber attacks".

Providing security can be seen in terms of the following cycle: (1) Protect: this involves 'system hardening measures', and anti-malware support for NATO projects. (2) Prevent: this means assessing and notifying vulnerabilities, as well as conducting training and awareness-raising. (3) Detect: using intrusion detection systems twenty-four hours a day, and checking incoming mail. (4) Respond: the teams must be ready to respond to incidents at any time of the day or night. (5) Recover: a recovery support service must be present, or available on-line, to ensure minimal disruption.

Case Studies: Estonia

Both this presentation, but particularly that of Ms Reet Oorn of the Estonian Informatics Centre, Tallinn, referred to the massive DDoS attacks on the Estonian government and institutions in April – May 2007. Ms Oorn gave a fascinating eye-witness account of how the Estonian government fought back against the attacks, when they were able to considerably increase their band width of their computers. The Estonians showed a united front, as government equipment was supplemented by that of private sector companies.

She also illustrated and discussed the results of the assessment conducted by her Informatics Centre. These showed that the attack was in two phases: an initial phase of attacks was on a small scale, and seemed to be designed to test the limits of the target computers. These attacks were associated with the 09 May WWII victory anniversary important to pro-Russian Estonians, who were already protesting violently about the prime minister's decision to remove a statue commemorating Russians heroes. The second phase was much more professionally organized, and hours of bombardments by bot-nets had clearly been purchased.

In terms of the success of the attacks, it is generally agreed that Estonia, which has some of the highest figures of internet use in the world, survived well. Two of the biggest banks in Estonia came under heavy DDoS attacks, and on-line services were unavailable for several hours. Attacks were also performed against critical routers at the Internet Service Providers level, and this disrupted the government's internet-based communication for a short time. Some government websites experienced temporary loss of service.

Can the Internet Be Given a Legal Framework?

Two speakers addressed the issue of whether legal controls can be imposed on the internet. Ms Eneken Tikk (Faculty of Law, Tartu University, Estonia), unlike Seymour Goodman, does not expect much of the UN: "One could argue that the method of developing legal instruments that the United Nations has used fails because it is too focused on building a consensus about … existing methods used by terrorists. It cannot lead the fight against new methods (such as cyber terror). Thus, we might consider using the United Nations experience as an argument to avoid an overly reactive (rather than proactive) approach …"

Ms Tikk's paper, "Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism", contains incisive comments on the main legal instruments concerning cyber attacks, relating these especially to terrorism. She addresses the Cyber Crime Convention (ETS No. 185), which, with the Convention on the Prevention of Terrorism (CETS No. 196), is "the most important international instrument for fighting cyber terrorism and other terrorist use of the Internet." However, not enough states are party to this agreement, weakening it considerably. Also, "serious threats to commit terrorist acts are not adequately covered either by this Convention … this Convention should be evaluated with regard to its ability to cover technological advances, particularly in the area of forensic investigative techniques (such as online searches or the use of key logger software). In the fast-paced technological environment of cyber crime, such evaluations, which frequently lead to revisions and updates, are an absolutely normal process, especially when dealing with high risks such as those posed by terrorism."

In general, like other lawyers at the Workshop, Ms Tikk warned that legal interventions in the internet might lead to infringements upon civil liberties. However, perhaps with the attacks on Estonia in mind, which led to almost no prosecutions, she added: "Should a decision to amend the Convention be taken, the possibility of excluding the political exception clause for some of the Convention's offences might also be considered, especially in serious cases of data and system interference."

The paper also gives details of amendments to the Estonian Penal Code, designed to strengthen the hand of prosecutors if similar attacks come. Estonian politicians also have an initiative at the EU level to amend the Framework Decision on Attacks against Information Systems 2005/222/JHA.

The other discussion of international law was offered by Police Superintendent Dr. Süleyman Özeren. The paper, "International Co-operation in the Global Response to Cyber Terrorism", presented the results of a comparative study concerning attempts to gain co-operation against the PKK and other terrorist groups like al-Qaida.

In cases where only one of the parties suffer from the terrorists' attacks, Dr. Özeren was very sceptical about the chances of gaining international co-operation in anything more than words. In practice, unless a country is being attacked, there is a lack of political will to implement co-operation agreements.

Terrorist Contents on the Internet

The papers mentioned so far have examined cyber terrorism in the proper sense of the term, and how to respond in terms of technology, awareness, and legal/political measures. However, there is also the related question of responding to the terrorist presence on the internet (so-called 'terrorist contents'). Here the internet is not a weapon, but an important tool for terrorists' communications (co-ordination, training, recruiting), and information gathering on the targets of planned attacks.

The COE–DAT Workshop included four fascinating papers on terrorist contents. An undoubted expert on terrorist websites is Prof. of Communication Gabriel Weimann, who from an early stage has been archiving literally thousands of terrorist websites, from al-Qaida to FARC, and Hizbullah to the PKK. His project, based at Haifa University, also brings many different analytical approaches to bear on this material, including link analysis, participant observation, language analysis, and case studies.

Prof. Weimann presented a report on his project called "WWW.al Qaeda: The Reliance of al Qaeda on the Internet". He shows how since 9/11, al Qaeda operatives sharpened their internet skills and increased their web presence.

When the Americans drove al-Qaida from its camps in Afghanistan, the organization was dispersed and forced to retreat into cyberspace. As Gabriel Weimann shows, they now make extensive use of the internet, even to the extent that they rely upon it. Also giving an account of a terrorist organization's use of the internet, Capt. Erdoğan Çelebi presented "A Case Study: the PKK and Cyberspace". Particularly interesting was the link analysis of the PKK-related sites, which was able to demonstrate which sites were used by PKK leaders in the field.

Responding to Terrorist Contents on the Internet

Other papers based on the phenomenon of 'terrorist contents' sought to give, in my view, very contrasting practical responses.

Yael Shahar, of the Institute for Counter Terrorism in Herzliya, Israel, spoke on "The Internet as a Tool for Intelligence and Counter-Terrorism". Yael Shahar notes that "The jihadi online presence is literally the physical brain of the global jihad movement. The very openness and accessibility of this medium provides the intelligence community with a wealth of material for foundation intelligence and analysis." Arguing that we should 'tune in' to, not try to shut down, these communications, she pointed out that much can be learned from analysis of websites and chat-rooms about the enemy's situation, plans, and also weaknesses.

Shahar is also interested in exploiting these weaknesses for counter-terrorism purposes, using the legally-shady method of 'hacking back', exploiting the same anonymity and access from which the terrorists benefit. She reveals an armoury of sowing dissent, countering propaganda, and secretly altering instructions on websites.

By contrast, Dr. Katharina von Knop proposes an open source response. Her discussion paper on the "Institutionalization of a Web-focused, Multinational Counter-terrorism Campaign – Building a Collective Open Source Intelligent System" focuses on the organizational and management issues surrounding such a system. She writes: "There is an intense need to work on new solutions to develop effective and efficient counterterrorism measures that follow the democratic process, values and freedoms. Knowledge discovery, data mining techniques and data fusion play a central role in improving the counter-terrorism capabilities of intelligence, security and law enforcement agencies... Having all the challenges in mind, this article will focus on the most important and highly sensitive one, international cooperation. This contribution … highlights the most important factors towards the development and institutionalization of an international interagency collective open source intelligent system regarding the threat of Islamist terrorism."

Dr. von Knop points out that, if such a co-operative campaign is to succeed, it will need to be arranged in an innovative and flexible way: instead of a hierarchical organization, there would be a network, and knowledge would be pooled. There would be committee management, and a credit point system. Governments would be allowed to use the resource only to the extent that they contribute good quality information and analysis.

Conclusion

The real value of the ARW was in the importance given by the speakers to practical responses to cyber terrorism. The contrasts in their methods both led to lively discussion in the Working Groups, but also raised the possibility of combined approaches. All the attendees, whether speakers or not, were able to gain a comprehensive view of the issues surrounding cyber terrorism.

Al-Qaeda's Religious Terrorism and the New Cold War

Çınar ÖZEN
Assoc.Prof.
International Relations Department, Gazi University

When Huntington introduced his "Clash of Civilizations" thesis, those that viewed this work in a scientific premonition-esque way comprised quite a large group. However, as time has gone by this perception has seceded its place to another view. Could the Clash of Civilizations have been offered to us as a new world strategy?

Huntington claimed that with the end of the Cold War civilizational differences would become the fundamental determinant of the world system. According to Huntington civilizations are comprised of large groups with a common denominator in culture, religion and identity. Huntington's clash of civilizations thesis hints especially at a potential conflict between democratic, liberal civilizations and Islamic totalitarian civilizations. In this light, the "other" for Western civilization after the Cold War was identified as Islamic totalitarianism. Many scholars who agreed with this view argued that Islamic Civilization should be expected to conflict with Western values because of its nature.

An important characteristic of the civilization concept is that it refers not to the state but to society. In that context a new larger society will be shaped up according to the civilizational line and replace the functional position of the nations in the international system as the main political actor. This shift, from nations to new larger civilizational societies will bring up a process of civilizational block formation and of ideological and political polarization. Civilizational approach reveals the weakening of the nation states and gradual disappearance of its primary actor status in the international system. The block formation in this new understanding of polarization will base on civilizational societies independent from nation states. This will indirectly impose on us the inevitable emergence of new political communities and actors according to the civilizational line. In this regard Huntington's approach implies the end of the Westphalian international system and the emergence of a new world order.

The second characteristic of the civilizational approach is that the civilization is not directly linked to political regimes. In other words not only the state but also the regime does not matter in that approach to explain the block structure of the international system. A civilization with an Islamic totalitarian culture, regardless of its regime type, will inevitably clash with Western values and ultimately with Western civilization. The clash of cultures, by definition is far removed from temporary political regimes and is rooted in permanent societal culture. In other words, civilizations with conflicting cultural values are bound to clash with one another.

After the 9/11 attacks, Huntington's analyses have gained momentum and strategies that utilize these views have become more widely accepted. However with the war that started on 9/11, in other words, the clash of civilizations, the other warring side is a terrorist group that operates on the basis of a transnational network. Viewed in this light, the concept of civilization is an especially useful concept to evaluate an enemy without a state organization and operating through a transnational network.

Al-Qaeda, is a terrorist organization using armed propaganda in search of a global world order. Many scholars see the ideological foundation of this organization in the "Ikhwan Al-Muslimoon" (Muslim Brotherhood) organization. The views of Sayyid Qutb of Ikhwan have especially had a formulative effect on Al-Qaeda's views. These views differ fundamentally from the Western democratic views in their understanding of sovereignty. According to Sayyid Qutb sovereignty belongs to God (*Hakimiyat Allah*). This presence of God's sovereignty necessitates that classes willing to rule society must find a divine will to legitimate themselves. Since the ruling class will be doing so in the name of God, they are also limited in their

accountability. In a way, this doctrine could be seen as an oligarchic class taking over power in the name of God.

Sayyid Qutb has also constructed a jihad ideology on top of this foundation. Within the framework of the World revolution of jihad ideology Muslims have been beckoned to fight for a new world order. The world order that Sayyid Qutb described is not very far from the understanding of the civilizational approach. In that world order Sayyid Qutb rejects the nation states as the essential actor of the international system. He rejects the national sovereignty concept as the political legitimacy instrument of the national and international poltical system as well. In that sense the world is conceived according to larger political communities and organizations differentiated from each other in respect to religion. More directly this differentiation means the Islamic world and the others. In this respect Huntington's civilization concept is replaced by religion based communities.

Al-Qaeda and related jihadist groups ideologicaly follow the Sayyid Qutb's interpretation of International politics. To conduct a global jihad for a new world order Al-Qaeda pursue a two-level war. In the first level Al-Qaeda, viewed in this light, has begun a struggle to establish regimes in the Islamic world where "sovereignty belongs to God". This domestic political level is essentially concentrated on the states where the majority of the population is Muslim and ruled by dictatorial regimes without having legitimacy in the eyes of its people. These poor and ignorant people suffering from dictators who have never experienced a fully functioning liberal democracy are close to accepting the ideology offered by Al-Qaeda as a progressive one in comparison to the dictatorships. Traditionally these communities are close to forming political communities according to religious elements. In that respect the failure of functioning nation-states with democratic regimes contributes to the reinforcement of the Al-Qaeda's ideology in these Islamic societies.

The second level of Al-Qaeda's war is on the international system level. On that level Al-Qaeda is searching for a new type of Islamic grouping in international politics and is in the midst of a war to break down the Western-centered world system. On that level Al-Qaeda targets Western communities. The terror offensives which target innocent people in Western societies are aimed at conducting the system level war of Al-Qaeda. These offensives aim to cause a clash in the communication channels between Western and Islamic societies. Al-Qaeda keeps assuring a degree of coordination between these two levels in that war. They expect to increase their power by keeping this coordination. Al-Qaeda has accomplished, with this coordination strategy, putting doubt in the minds of those that question the reality of the clash of civilizations thesis.

Al-Qaeda's war has another characteristic related with its transnational ideology. Al-Qaeda related groups are transnational actors behaving across the nations and states and use all the availabilities offered by the global system. In other words Al-Qaeda adapted itself very well to the conditions of the globalization. They use the structural weakness of nation-states in the age of globalization. The transnational character of Al-Qaeda terrorists, in that sense, is convenient for a war against nation-states and consistent with their global jihad ideology. In that context the developments regarding Al-Qaeda have begun to unravel that the clash is not at a state level but a war to create a new global order. The transnational characteristic of that war is explained in this phenomenon as well.

This is a strange war. On the one hand a transnational terror organization with global aims and its militants from various Islamic countries; on the other hand, a loose coalition of nation-states under US leadership. We should argue

that civilizational approach does not help the ideological struggle of the USA lead nation-states coalition to conduct the war against terror. On the contrary the Civilizational approach coincides with the ideological background of Al-Qaeda and creates counter productive effects on Islamic societies. Additionally civilizational approach creating fear and anger in the western society against Islam produce differentiation in the defining of the enemy. As a conclusion within the USA lead coalition this causes a clash of perception and attitude against Al-Qaeda and its ideological base.

It is not possible to argue that Al-Qaeda's armed propaganda on both levels has been successful. In other words Al-Qaeda is unsuccessful in its two-fronted war. The Islamic world is still bound to its national roots and not convinced of the reality of Islamic political communities. Al-Qaeda's threat upon the world system has never reached any serious levels that would warrant it to be taken seriously. Al-Qaeda's threat upon the world system should remain marginal as long as it continues to lack a strong state organization. The transnational methodology is not strong enough to convince Muslim populations that they live in a new unannounced cold war. On the other hand Al-Qaeda is quite successful to scare Western societies and to reignite hate against Islam. This can help to convince people that we live in a world where there is a clash of civilization. As this is stated at the beginning of this paper, the growing validity of the civilizational approach in the minds of the people will reinforce Al-Qaeda's ideology in the Islamic societies. This can have negative implications on the change of the political perceptions of the Islamic societies concerning the world and the order. This is where the real threat to world peace lies. The anti-Islamic currents taking effect in Western countries are making possible what Al-Qaeda never could with terrorism. Al-Qaeda's ideological foundation is not capable of achieving its ambitiousness. This foundation is only sufficient in persuading some fanatics to carry out acts of terror. The activation of these acts is only possible with the opportunities afforded to it by technology and with the financial support of certain circles. The global struggle against Al-Qaeda can only be successful by targeting the infrastructure of terror as opposed to an ideological struggle. There is a need to pay attention to not losing Islamic societies and the modern states that exist in the Islamic geography.

Religious Motivations For Terrorism

Julian CHARVAT
Maj (GBR A)
Course Director, COE-DAT

The modern world is one that faces many threats. Since the emergence of Al Qaeda throughout the 1990s and the horror of the attacks of 9/11 Terrorism has increasingly been the focus of the West's attention. In Afghanistan and Iraq there are significant troop deployments from many countries and daily fighting with casualties on all sides. There are still many thousands of volunteers who in some form or another support these terrorist activities and keep the organizations active. There are many reasons why someone may be attracted to a Terrorist cause and commit acts of hate and destruction. This article will discuss Religion as a motivation for Terrorism and examine how and why that creates different problems for those trying to combat it.

Terrorism can occur for a variety of reasons. A group may have a specific issue that it wants to change and bring the attention of the world to. These single-issue terrorists can be as violent for their causes as any other group but will usually only target those directly involved with their grievance. The Animal Liberation Front in the UK will target vivisection workers and the pro-life campaigners in the US have killed doctors who practice abortion.

Separatism is another major motivation for people to turn to Terrorism. This will generally be on a larger scale than the single issue terrorists and be more general it its targeting. This will usually be targeted at the general population and be content to cause more collateral damage. These groups will want to draw global attention to their perceived injustice as well as persuading the population to support their demands. The Liberation Tigers of the Tamil Eelam (LTTE) have recently even developed an air capability. The IRA and ETA have both conducted lengthy campaigns and in Turkey the PKK have been responsible for over 36000 fatalities during their activities. These terrorists do still differ from those whose motivation is religion. Religion is a motivator for some terrorists and probably the type of terrorism that comes to mind first in the modern world. Discussing religion is always a sensitive subject as for many millions it if the core belief in their life. It is important to acknowledge from the outset that the following discussion is about those who use religion to justify their terrorism. It is certainly not a discussion on these or any other religious belief.

A religion is more than a motivation to those who follow it. It will be the reason they live their particular lifestyle and effect how they view others. Followers will generally have a total belief in their views and regard others view as inherently wrong and misguided. Generally most religions talk of peace and love as their core beliefs and to not advocate violence. They will actively spread their message but will do so through education and information to convince non-believers that theirs is the true way. There are however fringes of the mainstream body who will believe that those not of their faith are lesser people and are a threat to them.

Religion alone is rarely the sole motivation for terrorism. Poverty, social injustice and state repression(1) are often drivers that push people from the mainstream but religion can be used to justify the criminal acts the commit.

For many terrorists the fact they are doing God's work is a major motivation for them. In some religions the followers believe themselves to be the Chosen People and regard others as being the enemies of God. The can focus on other races or religions specifically and will often regard the killing of the rest of the population as their path to salvation. This can lead them to want higher casualty numbers than other types of terrorist and give them reason to act. This also takes away the denial of escape or threat of capture as a deterrent. A person who believes they will gain

eternal paradise by killing and maiming themselves and others is not someone who can be reasoned with. It is therefore important to identify the religious motivations of terrorist groups as this will alter how they can be dealt with.

MESSIANIC CULTS

There have been many examples of small cults being formed who fanatically believe they are led by a new Messiah. These groups will follow the their leader without question and believe their only chance of salvation is by following their orders. One prominent example of this has been the Aum Shinrikyo cult in Japan. The cult believes that its leader, Shoko Asahara as a messianic figure and the group was formed to survive a catastrophic Third World War, which would begin in the USA. Michael Barkun describes the cult as "Forcers of the End"(2), the Cult believes there is an imminent Armageddon and they are obliged to occasion it to happen. The followers and members of Aum Shinrikyo believe they have to become superhuman through practicing a yoga technique and this would make them immune to biological and chemical agents.

The group began committing acts of violence of increasing ferocity during the 1990s. Their views that this would spark the Armageddon and bring their salvation meant that they had little regard for the human cost of their actions. If everyone else was about to die anyway why should they have a moral dilemma about their actions?

The group was responsible for one of the most infamous terrorist attacks pre 9/11 which highlights the added lethality from religiously motivated groups. In March 1995(3) Aum Shinrikyo attempted to release Sarin nerve agent on a crowded Tokyo underground. The attack killed 12 and injured over 5000. This was a clearly an attack that could only have been carried out by a religiously motivated group. The attack was fueled by their belief in the impending Armageddon and their own divine immunity to chemical agents and aptly demonstrated the higher potential lethality and disregard for others shown by religiously motivated terrorists.

The cult renamed itself Aleph and does not enjoy the membership or support it did during its peak and has been seen a massive crackdown on it from the Japanese authorities since 1995. It has been stripped of its religious status and the membership has dropped from 10000 to around 200(4).

CHRISTIAN IDENTITY MOVEMENT

The religion which motivates the terrorist will have an effect on their activity. Primarily in the US the Christian Identity Movements have been responsible for various terrorist acts. These may be smaller in scale and more localized that some other religiously motivated groups but do nevertheless present an example of terrorists acting in God's name. The Christian Identity Movement has been trying to propagate an anti-Semitic vision in the US(5).

The Christian Identity Movement has many off shoots and sub-organizations, which are all basically founded on 3 core beliefs. Firstly they believe that the Anglo-Saxon race is directly descended from the lost tribes of Israel mentioned in the Old Testament(6). They believe the Jews are directly descended from a relationship between Satan and Eve(7). Thirdly they believe the world is on the brink of Armageddon in which the Aryans must do battle with the Jewish conspiracy and their allies so that the world can be redeemed.

The Christian Identity movement includes elements of the Ku Klux Klan, the National Alliance and the Aryan Nations. Because these organizations have been very regional in their activities and not conducted the mass casualty attacks that the Aum Shinrikyo cult has in Japan their renown as a terrorist group is small, They have however carried out violent attacks on selected targets such as the attack on a Jewish Community Centre by Buford Furrow on August 1999 and his previous killing of Joseph Santos Ileto a postal worker killed as a target of opportunity by Furrow "because the mail carrier appeared to be Hispanic or Asian"(8).

Despite being relatively local these groups have the beliefs and intent to carry out larger attacks even though they currently do not have the drive and expertise to do so. Like the Aum Shinrikyo they believe in an Armageddon and their need to fight a struggle but the will target their victims on racial and religious lines and only accept casualties from those groups. Although currently still active these groups are more likely to carry out targeted crime but must not be forgotten as they have potential to grow again.

JEWISH SELF DEFENCE AND TERRORIST GROUPS

"So far as many people are concerned the principle role played by Jews in Modern Terrorist activity in the Middle East and elsewhere is that of victim(9)" There is however a long history of 'terrorism' leading up to the foundation of the Jewish State in 1948, As far back as Roman Times the Sicarii or Zealots would carry out broad daylight assassinations of Roman soldiers or Jewish citizens they believed guilty of betrayal(10). Later in the lead up to the creation of Israel groups such as Etzel and Lehi were influential to some degree in the withdrawal of the British and formation of an independent state. Given the turbulent geographical position and political situation around Israel it is not surprising that there is a Jewish Fundamentalist motivated terrorist groups.

The Kach party was founded by Rabbi Meir Kahane in 1971. Its ideology was based in his book "They Must Go" and espoused a doctrine that was militantly anti-Arab. The party called for the forced removal of Palestinians from the conquered areas of Israel such as the West Bank and Gaza Strip. He was assassinated by an Egyptian(11) in New York in 1990 and in 1994 his son Binyamin Zev founded the Kahane Chai (Kahane Lives) organization, which was proscribed as terrorist organization by both Israel and the USA(12). The organization carried out an attack on worshipers in the ar-Ibrahimi Mosque in 1994 which killed 29 Arabs. The group also has connections with Eyal who are associated with Yigal Amir, the assassin of Yitzahk Rabin.

Like the Christian Identity movements this group targets people on racial grounds and will accept mass casualties within that population. The will also target secular Jews as the do not follow the Jewish lifestyle to the beliefs of the Kahane Chai followers. Again their more regional activities has kept them in a lower profile than some other organizations. Even though they have had a higher lethality than Aum Shinrikyo(13) the have not attempted to use weapons of Mass Destruction and therefore not gained the coverage internationally but given their location and motivation they could project a far wider influence by inflaming a volatile situation.

AL QAEDA AND THE SALAFI JIHAD MOVEMENT

By the scale and target of their attacks in September 2001 Al Qaeda projected themselves and their cause into every Western media and consequently are probably the most infamous terrorist group today.

The Al Qaeda organization was formed by Osama bin Laden in the late 1980s after his time with Ayman Zaearhi's Makhteb al-Kihdmat in Afghanistan. This gave bin Laden the ability to create a network of radical Muslims and spread his ideas. His core beliefs are based around the absolute adherence to the Holy Koran and the creation of a pan-Islamic Caliphate.(14)

Bin Laden identified two 'battle fronts' to target. The close enemies are Muslim states who do not follow his extremist interpretation of Islam and the far enemy, effectively the USA and its allies.

The nature of Al Qaeda is different to more traditional terrorist groups. It is a network of loosely coordinated cells and has a horizontal rather than vertical hierarchy. It raises money from sympathizers worldwide and therefore his hard to target financially and is has a truly global reach.

Like most other religiously motivated terrorist groups Al Qaeda has a blatant disregard for human life other than devout Muslims. Moreover is sees the West as an evil that will corrupt good Muslims and therefore it not something that can be attacked, it is something that must be attacked.

The first significant attack by Al Qaeda was the failed bombing attempt of the World Trade centre in 1993. In 1998, two years after the Khobar Towers attacks the US embassies in Kenya and Tanzania were bombed. This showed that Al Qaeda was getting bolder and better in its attacks. The USS Cole was attacked by a suicide maritime bomber in October 2000 which was followed up by the massive attacks of September 2001. Since then the organization has been actively hunted by the Coalition but is has still achieved highly successful and lethal attacks in Istanbul, Madrid and London.

The cellular structure and horizontal hierarchy have meant that Al Qaeda and the Salafi Jihadists have been able to operate on a global scale and carry out attacks of an unprecedented nature. The religious motivation has given them a disregard for casualties and allowed them to try and kill huge numbers of civilians without warning.

The people who carry out these attacks are usually discontented young people who are recognized and groomed by the network. The often attend a religious school where they are taught absolute obedience to the Holy Koran and to hate those who do not do likewise. They are taught to believe that attacking the Kufir (non believers) is their duty and they will guarantee their place in Paradise by doing so.

Al Qaeda and the Salafi Jihad are currently active and planning future attacks. Much of their recent focus is centered in Iraq but their global network makes them a truly asymmetric threat.

THE EFFECT OF RELIGION ON TERRORISM

Clearly the problem of terrorism touches most religions and act of terror are carried out in their names. It is important to understand the religious aspects of a terrorist organization, as this will affect their targeting and lethality. For traditional terrorist groups, be they separatist, single issue or political they all have a set aim. In order to achieve this they will need some popular support and can not alienate the entire population.

They may cause considerable collateral damage and innocent casualties but they tend to target specific areas of people. The PKK's 2006 bombings of Turkish Holiday resorts were indiscriminate in their casualties but deliberate in their selection. The London attacks of 2005 showed that for a religiously motivated terrorist any target will do. When one of the 7/7 bombers had a problem with his detonator battery he could not get to his intended target, a Tube train, as he lost time buying a replacement. He then, on his own initiative, selected and blew up a bus. This shows that pure death and destruction were his aim without thought or care for the target.

DEALING WITH RELIGIOUSLY MOTIVATED TERRORISTS

Religion is based on faith and not scientifically demonstrated facts. It is therefore not something that can be freely and openly and dispassionately debated without offence. It also has an absoluteness that will cause its followers to be prepared to die for their beliefs or kill others for their disbelief. It also usually means that the terrorists do not have a set endstate that does not involve the total eradication of another way of life. It is important that the religion is not attacked when attacking the terrorists in order not to alienate the passive mainstream of the religion. Often the terrorist will try and cause this to happen to gain more support, an example being Al Qaeda promoting the concept of a new crusade with foreign troops in holy Islamic areas. This must be understood by those fighting terror so they do not reinforce this – Domke noted the increase Christian references of President Bush after 9/11 which may play into bin Laden's hands(15).

CONCLUSION

It is important to stress again that this article has discussed the use of religion by terrorists as a motivation and not discussed religion. The worldwide demonstrations after the publishing of the cartoon depicting the Prophet Mohammed or the Catholic reaction to Dan Brown's novel The Da Vinci Code show the depth of feeling this could cause. It is however important to understand the religious motivations of a terrorist group. It will affect their lethality and targeting as the will actively desire high casualty rates and do not court public opinion. They will also need to be dealt with in a sensitive way, not that the terrorists themselves should not face justice, but that any response must not alienate the religion. These can be quite interwoven and an understanding of the faith is required.

There are terrorist who are motivated by religion from almost every belief. Religion has played a part in separatist and single-issue terrorist activities too. One only has to look at Northern Ireland or a Pro Life terrorist act to see this. The job of fighting and dealing with the terrorist act may differ little – the reason behind the Sarin attack in Tokyo or the ar-Ibrahimi Mosque matters little to the incident responders but the strategy in combating the cause will.

BIBLOGRAPHY

Domke, David: God Willing, London, Pluto Press 2004

Bergen, Peter L: Holy War Inc., New York, Free Press, 2001

Weinberg, Leonard and Pedahzur, Ami (ed) Religious Fundamentalism and Political Extremism, Portland, Cass, 2004.

Harris, Sam: The End of Faith, London, Free Press 2004

Hoffman, Bruce: Inside Terrorism, New York, Columbia University Press, 2006.

Bodansky, Yossef: Bin Laden the man who declared war on America, Roseville, Prima Publishing 2001

Mamdani, Mahmood: Good Muslim, Bad Muslim, New York, Doubleday 2005

Burke, Jason: Al Qaeda, New York, I.B. Tauris, 2004

www.religioustollerance.org
www.jewishvirtuallibrary.org
www.janes.com.

References

(1) University of St Andrews CSTPV document Frameworks for Conceptualising Terrorism.
(2) Weinberg and Pedahzur (ed) pp63
(3) www.religioustollarance.org/dc_aumsh/htm
(4) www.tkb.org/Group.jsp?groupID=3956
(5) Barkun, Michael Religion and the Racist Right.
(6) www.religioustollerance.org.cr_ident.htm
(7) University of St Andrews CSTPV
(8) Burford Furrow quoted by cnn http://edition.cnn.com/us/9908/12/california.shootings.03/
(9) Arie Perliger and Leonard Weinberg in Weinberg, Leonard and Pedahzur, Ami (ed) Religious Fundamentalism and Political Extremism pp91
(10) Bruce Hoffman Inside Terrorism
(11)The assassin was acquitted but later convicted in connection with the WTC bombing
(12) www.jewishvertuallibrary.org
(13) Figures from religioustollerance.org
(14) Jane's World Insurgency and Terrorism 19 Aug 2005
(15) David Domke God Willing

Terrorism and The Media

Alexandru A. TEODORESCU
LTC (ROU A)
Instructor, COE-DAT

Julian CHARVAT
Maj (GBR A)
Course Director, COE-DAT

Introduction

The media is vital ground for terrorism, as the British Prime Minister Baroness Thatcher(1) said, "*publicity is the oxygen of terrorism*". Terrorism if far from random acts of violence, no matter how abhorrent the outcome, terrorists conduct attacks in order to further their particular cause or to draw attention to a perceived grievance. One certain by-product of their actions is publicity; in most free societies the media will report on the significant news events of the day. A successful terrorist attack against a high profile target, significant loss of life or even a successfully foiled plot uncovered by the police or security forces are likely to make the day's headlines. This will give the terrorist organisation publicity and bring their cause to the public's attention.

It is a conundrum for news agencies as to how they should report acts of terrorism. While the public has the right to know what is going on there is also a responsibility to avoid glamourising or glorifying the terrorists and their campaign. Due to the different regulations and ethics of media in different parts of the world when it comes to reporting terrorism and to the increasingly worldwide access to foreign media by satellite television, international press and the Internet it is very difficult to control the information and angle of reporting that people will see. It is therefore vital to understand the methods and trends in reporting terrorism and its portrayal in the media to effectively counter it with a well-managed and effective information campaign by those involved in the fight against terrorism. The Information War is an aspect of the battle space that must not be ignored or the battle for the will of the people may suffer. Terrorist organisations worldwide pay great attention to their portrayal in the media and will use this to gain maximum benefit for their campaign.

The freedom of the press is an inherent pillar in most democratic countries. This means that anything in the public interest may be published or broadcast by the media. This leaves governments with a difficult situation. If they pass laws to limit the media's freedom to deliver unbiased news relating to terrorism then they will leave themselves open to criticism that they are strangling the free press. This could backfire and lead to claims that the government is unjust and possibly raise the credibility of the terrorists who are attacking them. An example of this was during the Provisional Irish Republican Army's (PIRA) campaign against the British. In 1988 the British Government placed a ban on those representing PIRA from being allowed to speak on television. This was widely seen as a form of censorship and led to the ridiculous situation of the PIRA's Political Front Organisation, Sinn Fein's spokesman, Gerry Adams(2), being shown on television with an actor sound alike giving a voice over. This loophole in the banning legislation added failure to the accusation of censorship and the ban was repealed after a short time.

The Conundrum – Controlling The Media

In the modern world there are many competing media agencies all of which need to get the maximum number of viewers, listeners or readers. In order to achieve this they must deliver fast and thought provoking reports with insightful commentary on all major world events. They are almost all privately owned and therefore have the pressure of business added to their responsibility as journalists. This will also mean that the media will have a political bias and this is usually reflected in their reporting. Effectively the views of the owner and not necessarily the government or the people will dominate what and how events are reported.

To put controls on the media by the government is censorship. "Censorship is an anathema to most free societies."(3) This has many pitfalls and generally is frowned upon by all parties concerned. Although some countries have State Media, which is controlled by the government, there will almost always be private media giving different information. This may be a media that has responsible investigative journalists who seek to uncover the truth and bring it to public attention but may also have irresponsible journalists and editors who will put out a story that may sell copy or fill airtime regardless of the consequences of it.

Although the majority of the worlds media is independent that does not mean to say it is irresponsible. While the actions of an individual cameraman trying to get the best frame for his or her report or a reporter quoting out of context are irritating, it is the overall presentation of the event that must be judged. The balance between informing the public - a core duty of the media - and being a mouthpiece for terror is the balancing act the media must achieve. Censorship and government control is one method to ensure this occurs but the balance would be imperfect. If the government places tight control over what the media are allowed to publish the credibility of both is been eroded. Moreover, such restrictions can only be placed nationally and no matter how wide the embargo, the globalisation of international media will mean the censored view or reports will be available. However, voluntary regulation by the media is an acceptable method of safeguarding the democratic principle of a free media while showing responsibility by the broadcasters and publishers for the outcome of their reports.

Of course, given the media are free, this does not mean to say that self-regulation by the media should stop them running unpleasant or uncomfortable stories for the governments. Even in fighting terrorism the media is a reasonable check and balance on the actions of the security forces and the governments.

During the kidnappings in Iraq in 2003-2004 the media learned about the consequences of its broadcasts and reacted accordingly. Initially the first hostages were taken and videos were released showing them in orange jumpsuits, a clear reference to the detention centre at Guantanimo Bay. In these videos the hostage generally made a plea to his or her government and the terrorists would make a statement about their cause. These videos were well framed with specific backdrops to give a certain message to the viewer. Usually these videos were sent to the Qatari owned Al-Jazeera television company. Clips of these videos were widely shown and reported in the western media. Usually the hostages had several videos released before being murdered on a final video release, usually not shown by the responsible media but often available on the Internet. The media changed its position on the broadcast of these videos during the capture of the aide worker Margaret Hussain. Although the videos were released in the same way, the western media stopped showing them. Despite the fact that this did not actually save Mrs Hussain from murder, it did take away the reason the terrorist had conducted the kidnappings and killings. Thus, terrorists in Iraq soon abandoned this tactic, as it no longer provided them with the prize of publicity.

This act of voluntary self-regulation by the media demonstrated the power of publicity in the fight against terrorism. Clearly the method of reporting about the western citizens being captured and murdered in Iraq - as a matter of public interest that needs to be released - was the very fact that actually shaped events on the ground. The media learned from the situation, adapted and eventually acted responsibly to change the outcome.

Terrorist Broadcasts And Messages In The Mass Media

Most terrorist organisations seek the airtime and column inches of the media in order to promote their message. Very few media are likely to give unabridged, unedited access to anyone from a terrorist organisation, so the terrorists must use a method of release for their messages that is likely to make it into mainstream news. However, it is true that when reporting a terrorist message "media cannot help but illustrate in some way the message of the terrorist"(4).

Perhaps the best-known source of terrorist broadcasts is through the Qatari owned news agency Al-Jazeera. Formed in 1996 by the Emir of Qatar, Al-Jazeera set out to be the first truly independent Arabic language satellite news agency. Al-Jazeera also now broadcasts to many countries in English from a London studio. Al-Jazeera has a bureau in Baghdad and speaks the same language as most Al-Qaeda operatives in Iraq. It is therefore a natural choice for Al-Qaeda to contact if it has a video or recording to release.

Al-Jazeera has aired many videos and recordings from Al-Qaeda over the years. Further on, these videos are often reported and shown in part in the western media who are almost reporting the Al-Jazeera story. In fact in the West the majority of people will only have heard of Al-Jazeera because of it's airing of videos relating to Al-Qaeda. This has caused some to question Al-Jazeera as the medium through which bin Laden has been able to air his message.

Has Al-Jazeera been a platform for terrorist propaganda or has it acted with the same level (or lack) of responsibility as its western counterparts? Al-Jazeera has said that it will review each tape before it is aired and only broadcast them when they feel that it is suitable and that it is genuinely newsworthy. Part of the western criticism is that Al-Jazeera puts an eastern perspective on its broadcasts, which may differ from the standards and ideas the west regards as acceptable. Al-Jazeera is however showing no more bias in it's reporting than the Fox network would for a US perspective in its broadcasts.

The tapes themselves tend to be a well directed and planned product. The scene is set so the location is impossible to pin point and a great emphasis is placed on the symbology of the frame. Bin Laden has been often seen with maps of the world and weapons in the background, all designed to give the exact image he wants to portray. The message could be one for a call for Muslims to rise against the coalition in Iraq or to display the capability, strength and determination of his organization. Moreover, in one broadcast he even went as far offering a truce with Europe. Although such a message is itself newsworthy, airing it does influence those sympathetic to Al-Qaeda into action or further support. In addition, for the terrorists it may even contain a hidden trigger code to call a dormant cell into action. It is therefore an obvious risk in some respects for the media to broadcast them indiscriminately.

Al-Jazeera has drawn criticism from Washington and other western governments who have accused it of providing a mouthpiece for terrorism. It may be easier to raise these concerns about what is broadcast in the media when they do not have to make a call on censorship and prevent Al-Jazeera from reporting the Al-Qaeda tapes. One of the reasons that Washington may object to Al-Jazeera's coverage could be that it is uncomfortable with reporting, visualising, and portraying a different picture – readily available in western homes – than the one the official US and coalition would like to project to their populations.

Moreover, modern terrorism is more than ever focused on getting the psychological effects of it's acts to hit far beyond the immediate victims by intimidating or otherwise affecting the behaviour of a much wider target audience. Modern terrorists will maximise the psychological effects by effectively using the media to show tapes of their actions. This can range from unwittingly broadcasting terrorist messages to showing footage of a suicide attack. In order to utilise the mass media an their method of live broadcasts the modern terrorist will often select the timing and symbolic value of the target to maximise the coverage likely to be given to the attack. Thus, modern terrorism can be analysed in the effect it has on a wide audience far beyond those who are present at the scene of the event. The mass media holds the key for the terrorist's access to the world stage.

The Internet As a Media For Terrorists

The guidelines that set mass media activity may not be compulsory but most media agencies keep to them to gain the credibility of responsible reporters. Conversely, the Internet provides an easily accessible media vehicle to push out information and news propaganda genuinely without any regulation and constrictions. The meteoric rise of the Internet has meant that the potential for terrorist organisations to place their propaganda messages on the Internet is increasing all the time. Anyone with access to the web can set up an Internet site and is unrestricted on what they publish. Many terrorist organisations have used the Internet to allow supporters and sympathisers to read their message. It is also a medium for publishing material that the mainstream mass media shy away from. While most established media broadcast or published images from the murder videos of the Iraq hostages, refraining to show the actual decapitation, full footage including graphic images of the decapitations in detail was available within hours on the Internet. Thus, either by deliberate visitation or accidental surfing, the Internet provides a very simple method for the terrorist organisation to potentially reach millions.

In addition, it is not uncommon for Internet postings to alert the mainstream media to a story. However, this method of obtaining information means that they accept the risk of relaying on an unauthenticated and unregulated source.

Media Affecting The Story

Terrorism, unlike the ordinary crimes, is generally not a single one off incident(5). It is an ongoing campaign performed by a group with a cause or perceived grievances trying through violent means to get a government or population to accept its political views. There will be occasions where the terrorist organisation commits an attack that will last for a long time in the memory of the general public as a cause of concern. The Iraq hostage decapitation discussed above is an example of such an act and of how the media can have an effect. In hostage or hijacking situations the media reports may have a direct effect on the outcome of the situation. The safe release of the hostages often relies on a set of issued demands and the subsequent negotiations with authorities or their representatives. During this period it is essential that the negotiators have a confidential relationship with the hostage takers and that any compromise is kept quiet to save the face of those involved. If backed into a corner and faced with a widely broadcast situation, the hostage takers will often start to kill.

Undoubtedly the media has a right to report on a hostage situation or hijacking involving terrorists, but there are additional pitfalls in how they present their story. If they are broadcasting live from a scene there is the danger that the terrorists are watching or are in contact with someone watching the news and can see troop or law enforcement force disposition and movement. This could alert them about the authorities' potential tactical solutions and trigger them into a response. If the situation is ongoing for any length of time the media will start to speculate on all matters where they do not have fact. "Experts" will portray both the terrorist and security forces, and give their analysis of the likely outcome even though they have no actual information of the extraction plan. Again this might cause the hostage taker or hijacker to react or alert them to a possible method of attack. There will also be speculation on the demands. If the press report that a demand will certainly not be met it could take away the perception of credibility for the negotiator trying to broker a deal.

Two of the highest profile terrorist hostage takings and hijacks were directly influenced by the media handling of the story. In Munich in 1972 members of the pro-Palestinian terrorist organisation Black September attacked a dormitory full of Israeli competitors in the Munich Olympic Village. They took 9 of the Israeli team as hostages and killed 2 others in the process of the attack. Almost immediately the worlds press was broadcasting the event as it unfolded and the terrorist demand for the release of 236 Palestinian prisoners was made public before anyone in authority had time to examine the possibilities of dealing with the situation.

Negotiations ensued and their current status was broadcast by the media as it happened. The changes in the German position and the determination of the terrorists were broadcast to the world. Eventually a gun battle took place and 11 Israeli athletes, 5 terrorists and a German policeman were killed in total during the situation. It was felt by many that the media hindered the situation by being unhelpful and intrusive. For the terrorists it meant that some 900 million saw this happen on television(6). Other similar terrorist actions such as TWA 847 in 1985 have draw criticism for the media coverage of it.

Whatever the situation if it is ongoing it attracts a great deal of media interest. A terrorist attack makes a good story and fills the airtime or the copy the media require. It is how this is presented and what information is accurately given or speculated that possible affects the actual event in progress.

Summary

The relationship between the media and terrorism is mutually beneficial in some ways. While the media generally do not support terrorists they do give them and their cause the vital publicity that they strive. Conversely, the terrorist action makes a very interesting story and helps sell copy or draw listeners and viewers in great numbers. There is however a responsibility that comes with reporting these events. There is a danger that the media may inadvertently help the terrorists by publicising them and even broadcasting coded messages to terrorist cells/operatives. There is a fine line between legitimate public interest information – which the media is morally bound to publish – and glorifying the terrorists to some.

Censorship could ensure that the media are only showing safe and sterile material but this would also give the government too much control and remove the democratic principle of a free press. Media self-regulation solves the majority of problems but there are always agencies that go beyond the normal boundaries of acceptability or the unregulated Internet. In the modern *globalised* world of media, the different perspectives of different cultures may unavoidably make images or reports available that a government or nation finds uncomfortable.

Nevertheless, it is essential that the role of the media is understood and engaged by those fighting terrorism. If the media are ignored they will find information and run stories from other sources that may be wholly inaccurate and biased. In order to ensure the best relationship with the media, those who deal with public relations and Information Management must be seen at least as a force multiplier by those running the combating terrorism campaign. Airtime and press space is a competitive industry and if those fighting terror can beat the terrorist in this area of operations then the whole battle will benefit for it. Moreover, specifically due to these new challenges posed by the terrorist use of media and Internet and the significance of the "mind and hearts" battlefield, the Information Operation type of response – adaptively shifting from a supportive role, crafted to explain other physical measures, to a distinctively designed program, supported by other powers – may be even a more effective solution of combating terrorism than those developed and employed up to now.

Bibliography

Chermack S. Bailey F and Brown M: Media representations of September 11, Westpoint, Praeger, 2003

Coombs, Cindy C: Terrorism in the Twenty First Century, New jersey, Pearson, 2006

Greenberg, Bradley S (ed) Communication and Terrorism, Cresskill NJ, Hampton 2002

Norris P, Kern M and Just M (eds): Framing Terrorism, London, Routledge, 2003

Whittaker, David J: Terrorists and Terrorism, LONDON, Routledge, 2004

COE DAT Terrorism and the Media Course lecture summaries, Ankara, TGS 2007

References

(1) Baroness Margaret Thatcher was the British Prime Minister 1979 – 1990 during the main period of the Northern Ireland Troubles.
(2) Gerry Adams MP was leader of the PIRA political front organisation Sinn Fein. He was a Member of Parliament before and after the ban although he had lost his seat when the ban was in place.
(3) Coombs, Terrorism in the Twenty First Century, pp 154.
(4) Whitticker Terrorists and Terrorism pp 93
(5) Lone single-issue terrorists such as Timothy McVeigh, the Oklahoma bomber do exist but are not the norm for terrorism today.
(6) Whittaker, Terrorists and Terrorism pp 96 – 97

COE-DAT Activities

1 Chief of Turkish General Staff General Yaşar BÜYÜKANIT visited COE-DAT on 09 October 2007.

2 COE-DAT conducted a course on "Legal Aspects of Combating Terrorism" on 17-21 September 2007 in its facilities in Ankara/Turkey. During the course, legal response to terrorism in general, the concept of use of force, international treaties related to terrorism, human rights and terrorism, United Nations and terrorism, diverging national approaches to terrorism, legal aspects of cyber terrorism, interagency cooperation, future of legal aspects of combating terrorism, international operations against terrorism, legal aspects of funding of terrorism, military operations against terrorism and international law, London bombings in terms of legal aspects of terrorism were scrutinized. 58 participants from 20 different countries and 9 lecturers from 5 different countries have attended the course.

3 A workshop on "Responses to Cyber Terrorism" is held by COE-DAT on 4-5 October 2007 in Ankara/Turkey. Throughout the workshop, the history of internet, institutionalization of a web focused multinational counter terrorism campaign, critical information infrastructure protection, al-Qaeda and internet, types of cyber attack, international co-operation in the global response to cyber terrorism, internet as a tool for counter terrorism, NATO and cyber terrorism, cyber attacks with reference to Estonian case, and PKK's use of cyber space were discussed. There were 80 participants from 24 different countries and 12 lecturers from 6 different countries.

4 COE-DAT will conduct an Advanced Training Course (ATC) on "Organisational and Psychological Profile of Terrorism" on 22-26 October 2007 in Macedonia. By elaborating the aims and strategies of terrorist organisations, their recruitment methods, action methods and financial sources, the ATC aims to provide information about the structuring of terrorist organisations.

Concept Development and Experimentation Conference

5 2007 Concept Development and Experimentation Conference will be held between 5-8 November 2007 in Istanbul/Turkey. The conference is sponsored by SACT, USJFCOM and Turkish General Staff. COE-DAT is conducting host nation support activities on the behalf of Turkish General Staff. COE-DAT will also conduct a panel during the conference named "Deterrence of Terrorism- Prerequisites for Success."

6 COE-DAT will carry out the "Defence against Suicide Bombing Course" on 19-23 November 2007 at COE-DAT facilities in Ankara/Turkey. This course is conducted twice a year since the year 2005. The aim of this course is first to analyze the issue of suicide terrorism in different dimensions including the psychological, social, legal, financial, intelligence aspects and then to discuss how to defend against suicide attacks. The course is open to all NATO, Partnership for Peace (PfP) and Mediterranean Dialogue (MD) nations for participation.

7 COE-DAT is going to hold an international symposium in March 2008. The aim of the symposium is to provide a platform where different views and approaches concerning different dimensions of terrorism and counter-terrorism will be extensively discussed in order to develop a comprehensive common understanding of terrorism among nations.

In general, the symposium will focus on diverging national approaches to terrorism as well as the common international approach, the social and psychological dimension of terrorism, the present counter-terrorism, means, methods, concepts and doctrines together with the present and future needs and requirements, the legal aspects of countering terrorism especially in terms of international law, intelligence sharing and the importance of international cooperation in the fight against terrorism. The symposium is planned to address the presidents, heads of governments, ministries, head of international organizations and their representatives, high-ranking officers, their civilian equivalents, specialists, academicians and media.

COE-DAT

Centre of Excellence
Defence Against Terrorism

PK.57, 06582 Bakanlıklar
Ankara / TURKEY

Tel: 00-90-312-4258215
Fax: 00-90-312-4256489
E-mail: tmmm@tsk.mil.tr

www.coedat.nato.int

© **COE-DAT 2007** All Rights Reserved