



## CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM



# COE-DAT Newsletter

Volume 3 / Issue 15 / April-June 2010

## Content

### 3 General Overview of the Terrorist Activities (April - June 2010)

by Ergün ERÜN  
LTC (TUR AF)

Aslıhan AKYOL  
Data Base Manager (COE-DAT)

### 14 The Homeland Security Concept And its Applications in the United States

by Adil DUYAN  
LTC (TUR A)

### 28 Defence Against Terrorism

by Fevzi Birkal ÇUHADAR  
(1<sup>st</sup> Grade Police Chief)

by Tamer SERT  
Major (TUR GN)

### 38 Book Review

by Aykut ÖNCÜ  
Major (TUR A)

### 41 COE-DAT Activities

COE-DAT;

Your gate  
to get  
information.

## Editorial

**N**ewsletter's fifteenth issue has three main sections. First of all, we share the information and the analysis of the data related to the terrorist incidents which took place all over the world in the previous three months. Second, we have articles on terrorism related issues. Lastly, brief information about the activities of our centre is provided in the bulletin.

LTC Adil DUYAN, in his article on *The Homeland Security Concept and Its Applications in the United States of America*, focused on the notion of "homeland security" and how prominent it became in the United States (US) after 9/11 terrorist attacks. He explains how the scope of homeland security in US changed as well as the reflections on the structure of the Department of Homeland Security. Then he elaborates the essential sectors in homeland security: aviation security, maritime transportation security, border security systems/measures, public transportation security, preparedness-response-recovery, chemical security, food-bio security and bio terrorism, nuclear-radiological preparedness, information among agencies, laws

in homeland security, cyber security, media in homeland security relations, securing critical infrastructure and key assets.

Mr. Fevzi Birkal ÇUHADAR (1st Grade Chief of Police) and Maj. Tamer SERT share the findings of the *Defence Against Terrorism Course* via focusing on the concepts of history and causes of terrorism, the relationship among terrorism, security and democracy, legal aspects of terrorism, NATO DAT policy and structure, NATO's role in combating terrorism, WMD terrorism, cyber terrorism threat assessment, theology and the question of violence in religion, terrorism financing, organized crime and terrorism, media and terrorism, terrorist recruitment, crisis management and terrorism, the role of intelligence in combating terrorism, and strategic communication in combating terrorism.

Maj. Aykut ÖNCÜ reviewed the book on *Fighting the War on Terror: A Counterinsurgency Strategy*, authored by James S. CORUM and about the successes and failures of the US efforts in fighting against terrorism and insurgency.

TERÖRİZMLE MÜCADELE MÜKEMMELİYET MERKEZİ  
CENTRE OF EXCELLENCE - DEFENCE AGAINST TERRORISM



The opinions and comments in thi "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 (April - June 2010)

LTC Ergün ERÜN\*  
Aslıhan AKYOL\*\*

**I**n the second quarter of 2010 terrorist incidents increased roughly 24% and totaled 2,491<sup>1</sup> versus 1,998 from the first quarter of 2010. In this second quarter of 2010, 45 countries were afflicted with terrorist attacks versus 46 in the first quarter of 2010. 2,491 terrorist attacks resulted in 4,105 lives lost and 7,867 injured. Also, 648 people were abducted by unknown assailants during the period. The deadliest attack was an improvised explosive devices (IED) attack in India, West Bengal state, on May 28th. 100 people lost their lives in the Howrah-Mumbai Gyaneshwari Express derailment after landmine blast triggered by the Communist Party of India-

Maoist (CPI-Maoist) cadres between Khemashuli and Sardiha stations near Jhargram in West Midnapore District. Also, 200 people wounded in the attack.<sup>2</sup>

Another deadliest attack for the quarter was a suicide attack in Afghanistan, Kandahar province, on June 9th. A suicide bomber killed at least 84 people, a quarter of them children, and wounded 90 others at a wedding party. In the incident, a suicide bomber went inside the party where hundreds of people were sitting and blew himself up in Arghandab district, north of Kandahar. Many of the guests had links to local police or a militia that works with the Kabul government, which was why it was likely targeted.<sup>3</sup>



**IED attack in India claims 100 lives and 200 injuries on May 28<sup>th</sup>.**



**Suicide attacks in Kandahar province caused 84 dead and 90 wounded on June 9<sup>th</sup>.**

\* (TUR AF), Chief of Information Collection and Management Centre, COE-DAT.

\*\* Data Base Manager, Information Collection and Management Centre, COE-DAT.

<sup>1</sup> All figures mentioned in the report are totally procured from the open sources and any dispute in figures used in similar works is a matter of capability to reach the same source. Neither NATO nor COE-DAT is responsible for the disputes but the analyst.

<sup>2</sup> India Map, [http://newsimg.bbc.co.uk/media/images/39963000/gif/\\_39963279\\_west\\_bengal\\_map203.gif](http://newsimg.bbc.co.uk/media/images/39963000/gif/_39963279_west_bengal_map203.gif)

<sup>3</sup> India Map, [http://newsimg.bbc.co.uk/media/images/39963000/gif/\\_39963279\\_west\\_bengal\\_map203.gif](http://newsimg.bbc.co.uk/media/images/39963000/gif/_39963279_west_bengal_map203.gif)

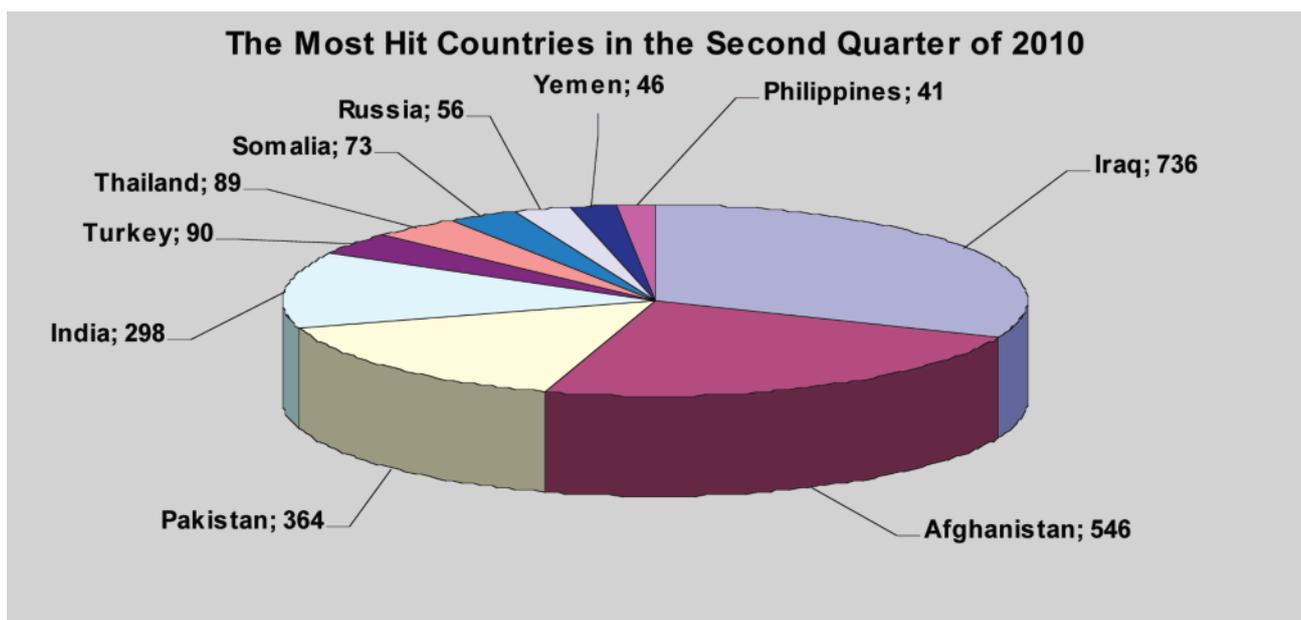
Iraq suffered by far the most with 736 separate attacks claiming 931 lives and injuring 3,029 others along with eight others abducted during the second quarter of 2010. The level of violence in Iraq increased roughly 13% according the previous quarter and accounts for 29% of total attacks, 23% of the total fatalities, and 39% of the total casualties for worldwide terrorist incidents. The capital city, Baghdad, saw the most attacks with 248 separate terrorist incidents, claiming 436 lives and wounding 1,625

people. The second most hit city in Iraq for the period was Mosul with 210 separate terrorist attacks. In Mosul, the attacks resulted in 176 deaths and 438 woundings.

The deadliest attack in Iraq was 23 April IED attack in Baghdad. The attack caused 54 people dead and more than 180 people wounded. The blasts targeted Shiite mosques. The death toll in Sadr City reached 39 killed and 56 wounded. Blasts in al-Amin area left eight people killed and 23 others wounded.<sup>4</sup>



**IED attacks in Baghdad claimed 54 lives and 180 injuries on April 23<sup>rd</sup>.**



<sup>4</sup> Iraq Map, (accessed October 25, 2005); available from <http://images.google.com.tr/imgress?imgurl=http://newsimg.bbc.co.uk>

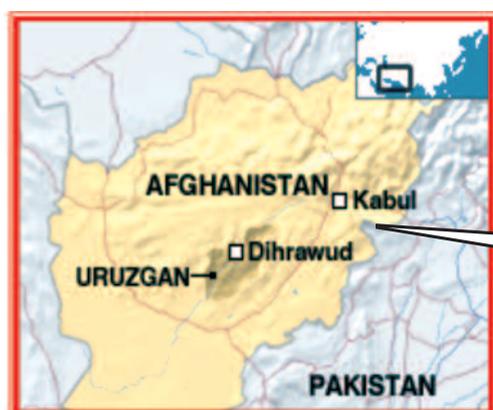
	Country	Event Count	KIA	WIA	AIA
1	Iraq	736	931	3,029	8
2	Afghanistan	546	954	1,264	32
3	Pakistan	364	704	960	99
4	India	298	465	327	27
5	Turkey	90	73	165	2
6	Thailand	89	59	445	0
7	Somalia	73	388	706	362
8	Russia	56	61	212	0
9	Yemen	46	95	76	17
10	Philippines	41	50	70	13

Table 1 - **The Most Hit Countries Worldwide during second quarter of 2010.**

In the second quarter of 2010 violence increased roughly 37% in Afghanistan. 546 attacks have recorded during the quarter versus 344 in the first quarter of 2010. These 546 attacks claimed 954 lives and injured 1,264 along with 32 people abducted during the period.

The deadliest attack for the second quarter of 2010 was a 23 April suicide attack in Kandahar province, claiming 84 lives and 90 injuries.

In addition, another suicide attack in capital city Kabul caused 18 dead and 47 wounded on May 18th. A suicide car bomber attacked a NATO-led military convoy during rush hour with a van packed with 750 kg of explosives. The attack was the deadliest strike against foreign troops in the heavily guarded capital since September 2009, when six Italian soldiers were killed by a car bomb. Most of the casualties were people waiting for a bus on the busy road near an army base.<sup>5</sup>



**Suicide attack in Kabul province claimed 18 lives and 47 injuries on May 18<sup>th</sup>.**



**IED attack in Khost province claimed 12 lives on April 28<sup>th</sup>.**

<sup>5</sup> Kabul map, available from [http://newsimg.bbc.co.uk/media/images/45040000/gif/\\_45040017\\_afghan\\_Kandabar\\_2209.gif](http://newsimg.bbc.co.uk/media/images/45040000/gif/_45040017_afghan_Kandabar_2209.gif)

<sup>6</sup> Khost map, available from [http://newsimg.bbc.co.uk/media/images/45080000/gif/\\_45040017\\_afghan\\_Khost\\_2208.gif](http://newsimg.bbc.co.uk/media/images/45080000/gif/_45040017_afghan_Khost_2208.gif)

In Pakistan violence increased 11% according to previous quarter. 364 terrorist incidents recorded during the second quarter of 2010 versus 322 in the first quarter of 2010. These attacks claimed 704 lives and causing 960 casualties along with 99 others abducted.

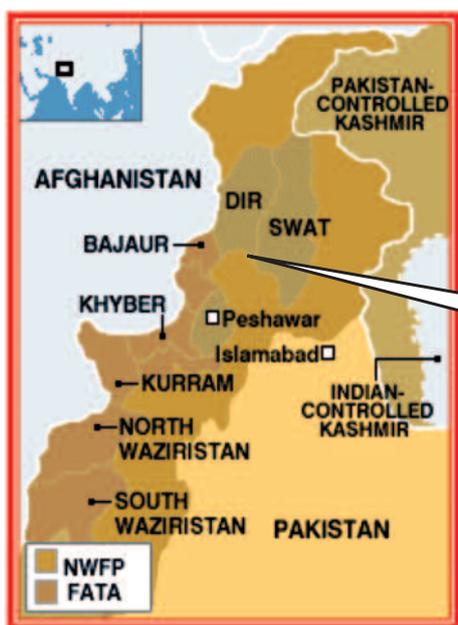
Suicide attacks decreased roughly 52% in Pakistan. 11 suicide attacks were recorded in Pakistan during the quarter versus 23 according to first quarter of 2010. Of these, 116 were killed and 285 were wounded in 11 suicide attacks.

The deadliest attack for the first quarter of 2010 was a multiple attack in Punjab province on May 28th. 80 people lost their lives and 92 others wounded in this attack. Gunmen attacked worshippers from a minority Muslim sect in two mosques of the eastern Pakistani city of Lahore, taking hostages and killing at least 80 people. Gunmen opened fire shortly after Friday prayers and threw grenades at two Ahmadi mosques in residential neighbourhoods in Pakistan's cultural capital. At least 80 people had been killed in the twin attacks in Garhi Shahu and Model Town. Also, a total of 92 were injured.<sup>7</sup>



**Multiple attack in Punjab province 80 lives and 92 injuries on May 28<sup>th</sup>.**

Also, another deadliest attack was a suicide attack in North-West Frontier Province (NWFP) on April 5th. At least 45 persons, including eight soldiers, were killed and more than 100 persons were injured. Suicide bomber targeted a rally of the Awami National Party (ANP) that rules the restive NWFP. The meeting was held at a rest house near the crowded bazaar in Lower Dir district.<sup>8</sup>



**Suicide attack in NWFP, Lower Dir district, claimed 45 lives and 100 injuries on April 5<sup>th</sup>.**

7 [http://newsimg.bbc.co.uk/media/images/41932000/gif/\\_41932036\\_pakistan\\_punjab2\\_map203.gif](http://newsimg.bbc.co.uk/media/images/41932000/gif/_41932036_pakistan_punjab2_map203.gif)

8 [Pakistan Map, http://newsimg.bbc.co.uk/media/images/45060000/gif/\\_45060447\\_pak\\_fata\\_nuf\\_226.gif](http://newsimg.bbc.co.uk/media/images/45060000/gif/_45060447_pak_fata_nuf_226.gif)

In addition, April 17 IED attack caused 44 people killed and 70 wounded. The target was Internally Displaced Person (IDP)'s camp in Kohat in northwestern Pakistan. One of the bombs went off at the registration point and the second blast occurred when people rushed to the scene to rescue the people.<sup>9</sup>

298 terrorism related violence put India in the fourth place in the world according to number of attacks carried out for the second quarter of 2010 again. These attacks claimed 465 lives and 327 injuries in sum along with 27 abducted by unknown assailants.

The deadliest attack was a 28 May IED attack, claiming 100 lives and 200 injuries, in West Bengal province.



**IED attack in NWFP, Kohat district, killed 44 people and wounded 70 others on April 17<sup>th</sup>.**

In addition, 5 April multiple attacks in central India, Dantewada district of the Bastar region, caused 76 policemen lost their lives. This was one of the worst attacks by the Maoist in years. The ambush by more than 700 Maoist fighters in Chhattisgarh state highlights the strong Maoist presence in India, especially remote rural areas.<sup>10</sup>



**CPI-Maoist killed 76 security personnel in Chhattisgarh on April 5<sup>th</sup>.**

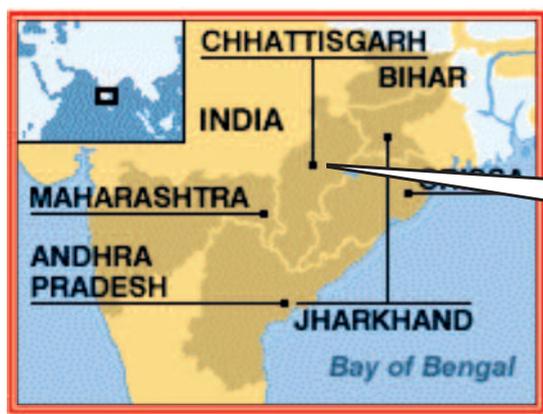
<sup>9</sup> Pakistan Map, [http://newsimg.bbc.co.uk/media/images/45060000/gif/\\_45060447\\_pak\\_fata\\_nwf\\_226.gif](http://newsimg.bbc.co.uk/media/images/45060000/gif/_45060447_pak_fata_nwf_226.gif)

<sup>10</sup> India Map, [http://www.bbc.co.uk/worldservice/images/2006/06/20060607105922india\\_states\\_map203.gif](http://www.bbc.co.uk/worldservice/images/2006/06/20060607105922india_states_map203.gif)

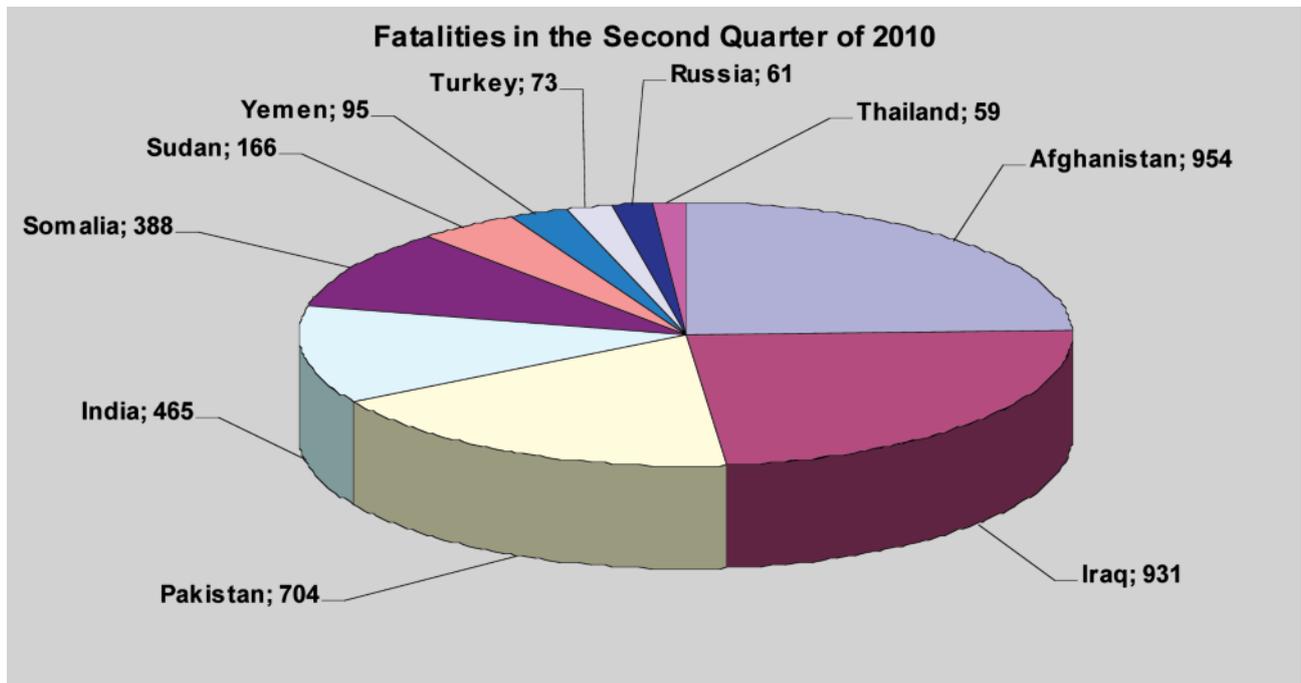
Also, another deadliest attack was a 17 May IED attack in Chhattisgarh again. The Communist Party of India-Maoist (CPI-Maoist) cadres killed 45 persons when they blew up a bus by triggering an IED at Chingavaram near Sukma in Dantewada District on May 17. There were around 32 civilians and 18 SPOs in the bus.<sup>11</sup>

90 terrorism related attacks made the Turkey the most fifth targeted country in the world during the second quarter of 2010. These attacks claimed in 73 lives and 165 injuries along with two abducted.

The most deadly incident was a June 19 clash. In the clash eight soldiers martyred and 14 others wounded in Hakkari. In addition, another deadliest terrorist attack occurred in Hatay. Indirect Fire (IDF) attack in Hatay caused six soldiers martyred and seven others wounded on May 31st.



**CPI-Maoist killed 45 security personnel in Chhattisgarh on May 17<sup>th</sup> by triggering IED.**



<sup>11</sup> India Map, [http://www.bbc.co.uk/worldservice/images/2006/06/20060607105922india\\_states\\_map203.gif](http://www.bbc.co.uk/worldservice/images/2006/06/20060607105922india_states_map203.gif)

PKK/KONGRA-GEL terrorists used six different methodologies during the quarter, and the most prevalent one was IED attacks with 41 repetitions, claiming 22 lives and 71 injuries, while clash was the second most-used tactics with 22 incidents, causing 25 dead and 44 wounded. Also, 15 armed attacks resulted in 10 deaths and 27 woundings, while three IDF attacks claimed six lives and eight injuries. In addition, three arson attacks caused no casualties. Lastly, two civilians were abducted in Hatay on June 8th.

Thailand was the sixth most hit country in the second quarter of 2010. 89 terrorist attacks caused 59

people dead and 445 others wounded. Three troubled southern provinces, Pattani, Narathiwat and Yala were the most volatile cities in terms of the number of attacks carried out during the quarter. Pattani suffered 20 attacks that resulted in 16 people killed and 79 others wounded while in Yala eight people were killed and 129 were wounded in 16 separate attacks. The province of Narathiwat also suffered a significant number of attacks, 16, which claimed 18 lives and wounded 28. The largest attack was 1 April armed attack in Narathiwat province.<sup>12</sup> Insurgents trapped a pick-up truck and opened fire at it before setting it on fire, killing three men and injuring another.



**Armed attack in Narathiwat province caused six dead on April 1<sup>st</sup>.**



**Suicide attack claimed 45 lives and 100 injuries in Mogadishu on May 1<sup>st</sup>.**

73 terrorist attacks made the Somalia the most-hit seventh country in the world during the second quarter of 2010. 73 attacks claimed 388 lives and 706 injuries including 362 others abducted. The deadliest attack was 1 May suicide attack in capital city Mogadishu, claiming 45 lives and 100 injuries.

<sup>12</sup> Pattani map, available from [http://newsimg.bbc.co.uk/media/images/40090000/gif/\\_42762191\\_india\\_pattani\\_map203.gif](http://newsimg.bbc.co.uk/media/images/40090000/gif/_42762191_india_pattani_map203.gif)

Eight different tactics used by terrorist in Somalia during the period, and the most used one was clash with 23 repetitions, killing 240 people and wounding 471 others, while piracy was the second most-used methodology with 23 repetitions, claiming one life and one injury along with 362 abducted. IED was the most-used third methodology with 10 attacks, resulting in 43 deaths and 69 woundings. Indirect fire (IDF) attack was the most used fourth tactic with eight separate incidents, claiming 45 lives and 60 injuries in sum. Other tactics used in Somalia were armed attack, execution, raid and suicide attack during the quarter.

Violence in Russia continued in the second quarter of 2010 and increased roughly 38%. 56 separate terrorist incidents versus 35 according to previous quarter, resulting in 61 deaths and 212 woundings.

The most significant attack in Russia was 13 May IED attack in Dagestan. IED attack in Dagestan caused eight people dead during the quarter, while another deadliest attack on May 26, claimed seven lives and 40 injuries.

IED Attack, including six vehicle-borne improved explosive devices

(VBIED) attack, was the most used tactic during the quarter with 24 occurrences, while armed was the most used second tactic with 12 occurrences in Russia. Also, eight clashes and three suicide attacks occurred. Other methodologies used in Russia hoax, IDF and raid during the quarter.

Yemen was the most hit ninth country in the world during the second quarter of 2010. 46 separate terrorist attacks claimed 95 lives and 76 injuries including 17 others abducted. The most deadly attack was 25 June clash, claiming 11 lives. Seven different methodologies used by terrorists during the period and the most used one was armed attack with 14 repetitions, resulting in 19 deaths and eight woundings, while clash was the most-used second tactic with 13 attacks, causing 48 dead and 47 wounded. Also, abduction, IED attack, raid, suicide attack and VBIED attack were the other methodologies used in Yemen during the period.

The violation increased roughly 34% in Philippines and some 41 attacks claimed 50 lives and wounded 70 people along with 13 people abducted during the second quarter of 2010. The deadliest attack was 11 May armed attack in



**IED attacks in Dagestan province claimed eight lives on May 13<sup>th</sup>.**

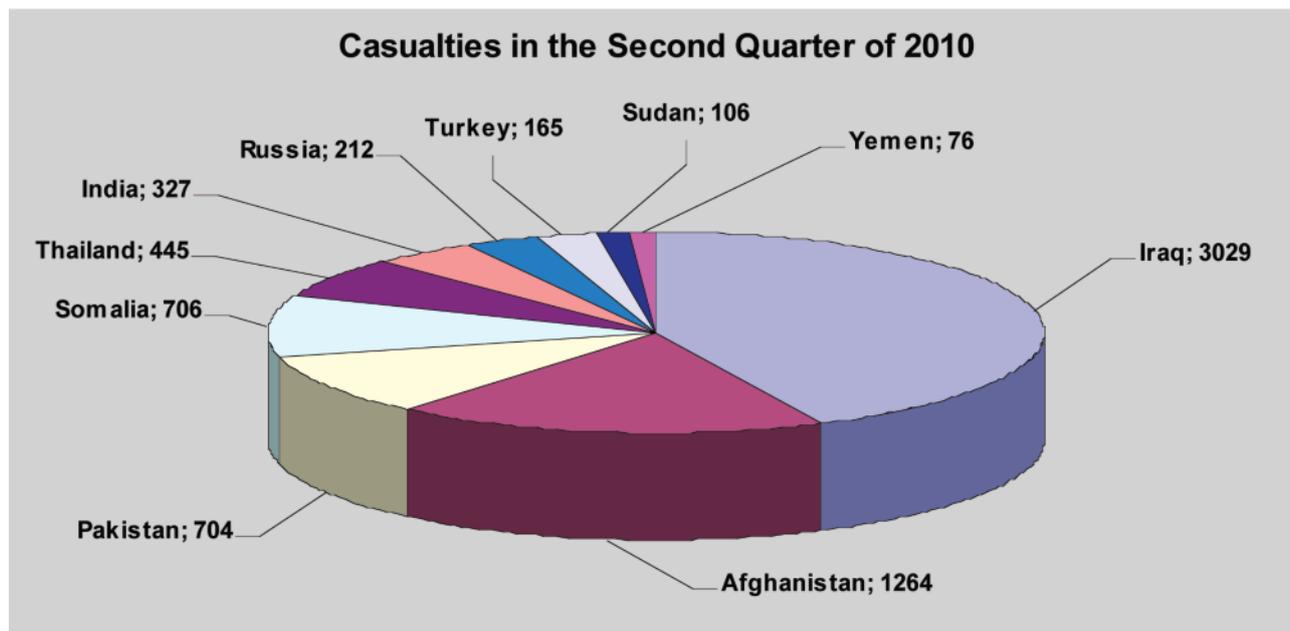
Mindanao province, claiming six lives and 12 injuries. In terms of methodology, clash was conducted 12 times resulting in 13 deaths and 19 wounded, while armed attack occurred 10 times and caused 22 dead and 26 wounded. In addition, five IED attacks including one VBIED attack claimed five lives and 12 injuries while five IDF attacks resulted in four deaths and eight woundings. Also, two raids resulted in four deaths and five woundings, while two civilians executed. Lastly, 13 people were abducted in Philippines in different five abductions during the quarter.

Lastly, in Europe six countries were hit by terrorists during the quarter including Turkey and Russia. The most hit country was Turkey with 90 separate attacks while Russia was the second one with 56 separate attacks. Also, Bosnia and Herzegovina (BIH), FYROM Macedonia, Greece and United Kingdom (UK) were the other

countries suffered from terrorism during the period.

Terrorists used 13 different tactics in the second quarter of 2010. IED attacks were the most used tactic during the quarter with some 907 attacks, claiming 1,174 lives and 3,065 wounded, while traditional armed attacks were the most used second tactic during the quarter with some 575 repetitions, resulting in 882 deaths and 384 woundings along with one abducted. Iraq was the most targeted with IEDs, suffering 368 separate attacks. Afghanistan was the second country suffered IED attacks with 243 incidents while Pakistan was the third most targeted country with 73 incidents. Lastly, 73 IED attacks reported from India while 41 IED attacks were reported in Turkey. The deadliest IED attack was 28 May IED attack in West Bengal state in India. At least 100 people were killed and 200 others wounded in the incident.

**Casualties in the Second Quarter of 2010**



	Event Type	Event Count	KIA	WIA	AIA
1	IED	907	1,174	3,065	0
2	Armed Attack	575	882	384	1
3	Clash	379	861	1,250	2
4	IDF	163	131	572	0
5	VBIED	125	185	859	0
6	Suicide Attack	79	495	1,397	0
7	Abduction	78	12	4	232
8	Raid	68	254	321	17
9	Execution	55	99	0	0
10	Arson	27	0	0	0
11	Piracy	26	1	1	396
12	Hoax	4	0	0	0
13	VOIED	2	11	14	0

Table 2 - **The Most Used Tactics in the World during the Second Quarter of 2010.**

Extrajudicial killings posed an important security challenge for Afghanistan, India, Nepal, Pakistan, Philippines and Somalia and especially for Iraq where 128 people lost their lives in captivity in 60 separate incidents during the first quarter of 2010.

Clashes between security forces and terrorists caused considerable damage. 379 incidents claimed 861 lives and 1,250 injuries along with two abducted.

A wide usage of Indirect Fire (IDF) attacks was also noted during the quarter, killing 131 and wounding 572 in 163 attacks.

Another deadly IED tactic, the vehicle-borne improved explosive devices (VBIED) attack, was the

fifth most used tactic. There were 125 separate attacks claiming 185 lives and injuring 859 during the quarter. Iraq was the most afflicted with 95 separate VBIED attacks that killed 157 people and wounded over 698 others. Other countries with attacks using this tactic during the quarter were Afghanistan, Iran, Nepal, Pakistan, Philippines, Russia, , Thailand, UK, USA and Yemen.

Suicide Bombing was the deadliest form of IED attack again with 79 incidents killing 495 people and wounding 1,397 others during period. Afghanistan was the most volatile country according to data available about suicide attacks with 37 separate attacks, while Iraq was the second most suffered country from suicide attack with 21 of these attacks. Pakistan was the third hardest hit by this tactic, suffering 11 such attacks. Other countries targeted were Russia with six, Somalia with two and Yemen afflicted with two attacks during the quarter.

Abductions were another tactic used during the period. Some 78 attacks killed 12 people and wounded four. In addition, assailants kidnapped 232 people during the first quarter of 2010.

Raid was the most used eighth tactic during the period with some 68 separate attacks, claiming 254 lives and 312 wounded along with 17 abducted. Afghanistan was the most hit country with 22 separate raid attacks while Pakistan were the second most hit country with seven attacks. In addition, Algeria, Democratic Republic of Congo (DRC), India, Iraq, Kenya, Nepal,

Niger, Philippines, Russia, Somalia, Sudan, Thailand, Turkey and Yemen were the other countries afflicted raid during the quarter.

Execution was the tenth most used tactic during the quarter with some 55 attacks, claiming 99 lives. Iraq was the most volatile country related to execution with 18 incidents, resulting 32 deaths. Also, Afghanistan, India, Nepal, Pakistan, Philippines and Somalia were other countries where execution occurred during the period.

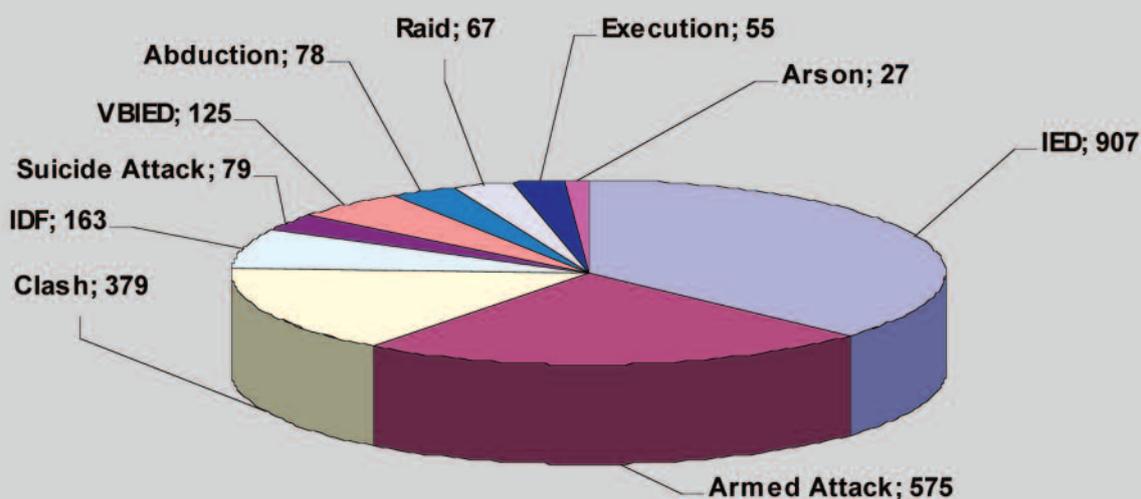
During the quarter 27 arson attacks caused no casualties. India

was the leading country with 15 arson attacks. Also, Pakistan, Thailand and Turkey were the other countries afflicted arson attacks.

The victim-operated improvised explosive device (VOIED) attack was the thirteenth most used tactic for the period with two attacks claiming 11 lives and injuring 14 during the quarter. India and Thailand were the countries afflicted VOIED attack during the second quarter of 2010.

Lastly, 26 piracies, four hoaxes were reported during the second quarter of 2010.

**The Deadliest Tactics Used in the Second Quarter of 2010**



## The Homeland Security Concept and its Applications in the United States

LTC Adil DUYAN\*

The term became prominent in the United States of America (USA) following the September 11, 2001 attacks; it had been used only in limited policy circles prior to these attacks. The phrase “security of the American homeland” appears in the 1998 report *Catastrophic Terrorism: Elements of a National Policy* by Ashton B. Carter, John M. Deutch, and Philip D. Zelikow. Homeland security is an umbrella term for security efforts to protect the United States against perceived internal and external threats. The term arose following a reorganization of many U.S. government agencies in 2003 to form the United States Department of Homeland Security after the September 11 attacks, and may be used to refer to the actions of that department. The term is currently not in use in any other country. Homeland security is also usually used to connote the civilian aspect of this effort; “homeland defense” refers to its military component, led chiefly by the U.S. Northern Command headquartered in Colorado Springs, Colorado.

The scope of homeland security in USA includes emergency preparedness and response (for both terrorism and natural disasters), including volunteer medical, police, emergency management, and fire personnel; domestic intelligence activities, largely today within the FBI; critical infrastructure protection; border security, including both land and maritime borders; transportation security, including aviation and maritime transportation; bio-defense;

detection of radioactive and radiological materials and research on next-generation security technologies. Today in the updated structure of Department of Homeland Security (DHS), there are 30 sections. Before 9/11, all of them were under different structures. As a result of the Homeland Security Act of 2002, Title I - Department of Homeland Security Sec. 101. Executive Department says that;

(a) Establishment. - “There is established a Department of Homeland Security, as an executive department of the United States within the meaning of title 5, United States Code.

(b) Mission

In General. - The primary mission of the Department is to

- Prevent terrorist attacks within the United States;
- Reduce the vulnerability of the United States to terrorism;
- Minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States.”

However, some homeland security activity remains outside of DHS; for example, the FBI and CIA are not part of the Department, and other agencies such as the Department of Defense and Department of Health and Human Services play a significant role in certain aspects of homeland security. Homeland security is coordinated at the White House by the Homeland Security Council. The National Strategy for Homeland Security, October 2007.

Homeland security is officially defined by the National Strategy for Homeland Security as “a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur”. Because the U.S. Department of Homeland Security includes the Federal Emergency Management Agency, it also has responsibility for preparedness, response, and recovery to natural disasters.

Main sectors in “Homeland Security” may change according to the country or due to specific conditions in that country. But these following sectors are essential to be considered if we are going to talk about the comprehensive concept of “Homeland Security”: Aviation Security, Maritime Transportation Security, Border Security Systems/Measures, Public Transportation Security, Preparedness-response-recovery, Chemical Security, Food-Bio Security and Bio terrorism, Nuclear-Radiological Preparedness, Information among Agencies, Laws in Homeland Security, Cyber Security, Media in Homeland Security Relations, Securing Critical Infrastructure and Key Assets.

### **1. Aviation Security**

Aviation security is the first to talk about. On the 11th of September, attacks came by air. The concept of “Homeland Security” was born. National Security Presidential Directive details a strategic aviation security. 6 supporting plans address the following areas; the coordination and integration of

government-wide aviation security efforts, the strategy sets forth government agency roles and responsibilities, establishes planning and operations coordination requirements, and builds on current strategies, tools, and resources.

There are “6 main plans” to overcome the terrorist threat. Aviation Transportation System Security Plan seeks to enhance public security and economic growth by promoting global aviation security practices aimed at reducing vulnerabilities associated with the aviation transportation system. If we mention four them, the first one is “Aviation Operational Threat Response Plan” (ATSR Plan) ensures a comprehensive and coordinated government response to air threats. “Aviation Transportation System Recovery Plan” ensures rapid recovery from an attack or similar disruption in the Air Domain. The ATSR Plan includes recommended measures to mitigate the operational and economic effects of an attack in the Air Domain. “Air Domain Surveillance and Intelligence Integration Plan” (The ADSII Plan) is a plan to coordinate requirements, priorities, and implementation of air surveillance resources and the means to share this information with appropriate stakeholders. The ADSII Plan supports an enhanced surveillance capability to detect and deter threats that could lead to an attack on the aviation transportation system. “Domestic Outreach Plan” (The DO Plan) include coordination with State and local

government authorities and consultation with appropriate private sector persons and entities. The DO Plan ensures that this proper coordination with the private sector and local government authorities takes place. “International Outreach Plan” (The IO Plan) efforts must be global efforts and developed with the cooperation of other governments and international organizations. The IO Plan is aimed at ensuring the proper coordination with entities abroad.

There are some “concrete projects” for “Aviation Security”. For example “Secure Fixed Based Operators” (FBO) would allow for FBOs to check manifests against “Electronic Advance Passenger Information System” (eAPIS) filings to better identify the flight crew and passengers on board general aviation aircraft. “Preliminary” is an agreement which broadens U.S. Customs and Border Protection (CBP) operations in Shannon and Dublin, Ireland, to include full preclearance of commercial and private air passenger flights destined for the U.S. Private aircraft flying through Ireland may use CBP preclearance facilities to fly to any airport within the U.S., without having to stop at a pre-designated airport of entry for customs clearance before continuing to their final destination. “Electronic Advance Passenger Information System” brings additional measures to strengthen private aircraft security by requiring more detailed information about arriving and departing private aircraft and persons onboard, within a timeframe necessary for the

Department to assess. “Radiation/Nuclear Detection Screening” is to identify key vulnerabilities to weapons of mass destruction threats, specifically with regard to radioactive and nuclear items. DNDO, together with “Customs and Border Protection” (CBP) and Transportation Security Administration (TSA), is working to facilitate international general aviation operations while enhancing security all international general aviation aircraft are scanned upon arrival to the U.S. using handheld Radiation Isotope Identification Devices (RIID) by CBP officers. These measures are part of a much larger initiative to create a Global Nuclear Detection Architecture to protect country from radiological and nuclear threats whether they come by land, air, or sea.

## **2. Maritime Transportation Security**

Maritime domain is defined as “All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances”. To protect this maritime domain, “8 supporting plans” have been created; there are several technical details concerning each plan. For example, “Maritime Commerce Security Plan” establishes a comprehensive plan to secure the maritime supply chain. “Maritime Infrastructure Recovery Plan” recommends procedures and standards for the recovery of the

---

maritime infrastructure following attack or similar disruption. “International Outreach and Coordination Strategy Plan” provides a framework to coordinate all maritime security initiatives undertaken with foreign governments and international organizations, and solicits international support for enhanced maritime security. “Global Maritime Intelligence Integration Plan” uses existing capabilities to integrate all available intelligence regarding potential threats to U.S. interests in the maritime domain.

Here, it is important to talk about the “Container Security Initiative” (CSI). CSI addresses the threat to border security and global trade that is posed by potential terrorist use of a maritime container to deliver a weapon. CSI uses a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. Through CSI, CBP officials work with host customs administrations to establish security criteria for identifying high-risk containers. Those administrations use “non-intrusive inspection” (NII) and radiation detection technology to screen high-risk containers before they are shipped to U.S. ports.

The three core elements of CSI are; to identify high-risk containers (CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence), to prescreen and evaluate containers before they are shipped (containers are

screened as early in the supply chain as possible, generally at the port of departure) and to use technology to prescreen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade (this technology includes large-scale X-ray and gamma ray machines and radiation detection devices).

Currently, approximately 86 percent of all maritime containerized cargo imported into the United States is subjected to prescreening. CSI continues to expand to strategic locations around the world. The World Customs Organization (WCO), the European Union (EU), and the G8 support CSI expansion and have adopted resolutions implementing CSI security measures introduced at ports throughout the world.

### **3. Border Security Systems/ Measures**

Security forces in all countries are working to strengthen security on the borders to disrupt the drug, cash and weapon smuggling that fuels cartel violence adding manpower and technology to the borders. The trend after 9/11 is to support smart security on the border and to facilitate international travel and trade. Borders & Maritime Security Projects are still under way. These projects below are developed to help enhance the security of borders and waterways without impeding the flow of commerce and travelers.

These are “Advanced Container Security Device Project”, “Advanced Screening and

Targeting Project”, “Air Cargo Composite Container Project”, “Automatic Target Recognition Project”, “Border Officer Tools Project”, “Border Officer Safety Project”, “Bordertech Project”, “CanScan Project”, “Container Security Device Project”.

As an example, “Advanced Container Security Device Project” (The ACSD) is developing an advanced sensor system for monitoring the container’s integrity from the point of consolidation to the point of deconsolidation in the maritime supply chain. The ACSD is a small unit that attaches to the inside of a container to monitor all six sides of the container to report any intrusion or door opening. It will also detect the presence of human cargo in the container. If ACSD detects an intrusion, breach, door opening or human, it will transmit this alarm information through the Marine Asset Tag Tracking System (MATTS) to United States Customs and Border Protection. The ACSD will also build in a standard plug-and-play interface capability so that other security or commercial sensors (e.g., radiological/nuclear, chemical/biological) can be easily integrated through the standard interface. The ACSD must be able to withstand the harsh environmental conditions of global shipping and be economical for shippers to use.

Another example is “Automatic Target Recognition Project” (ATR). Automatic Target Recognition Project develops an automated imagery detection capability for anomalous content (e.g. persons, hidden compartments, contraband)

to be integrated with existing and future (i.e., CanScan) non-intrusive inspection (NII) systems. This ATR capability is broadly applicable to the scanning and imaging systems providing an operator-assisted decision aid for target discrimination within low-resolution images. Further, the ATR will be scalable to accommodate advanced NII systems with higher resolution imagery and material discrimination capability.

#### **4. Public Transportation Security**

In transportation system, there are “6 key subsectors”. “Aviation Transportation System” includes aircraft, air traffic control systems, commercial airports, additional airfields. This mode includes civil and joint use military airports, heliports, short takeoff and landing ports, and seaplane bases.

“Maritime Transportation System” consists of coastline, ports, navigable waterways, “Economic Zone” to secure, and intermodal landside connections, which allow the various modes of transportation to move people and goods to, from, and on the water. “Highway” encompasses roadways and supporting infrastructure. “Vehicles” include automobiles, buses, motorcycles, and all types of trucks. “Mass Transit” includes multiple-occupancy vehicles, such as transit buses, trolleybuses, vanpools, ferryboats, monorails, heavy (subway) and light rail, automated guide way transit, inclined planes, and cable cars designed to transport customers on local and regional routes. “Pipeline Systems” include vast

---

networks of pipeline that traverse hundreds of thousands of miles throughout the country, carrying natural oil, gas and hazardous liquids, as well as various chemicals. “Rail” consists of hundreds of railroads, more than 143,000 route-miles of track, more than 1.3 million freight cars, and roughly 20,000 locomotives.

So, the “Transportation Systems Priority Programs” driven by overall sector goals are; to prevent and deter acts of terrorism using or against the transportation system, to enhance the resiliency of transportation system and to improve the cost effective use of resources for transportation security.

### **5. Preparedness, Response, Recovery**

In the preparedness system, the purposes are; to organize and synchronize national (including federal, state, local, tribal, and territorial) efforts to strengthen national preparedness; guide national investments in national preparedness; incorporate lessons learned from past disasters into national preparedness priorities; facilitate a capability-based and risk-based investment planning process; and establish readiness metrics to measure progress and a system for assessing overall preparedness capability to respond to major events, especially those involving acts of terrorism.

“The National Planning Scenarios”, which depict a diverse set of high-consequence threat scenarios of both potential terrorist attacks and natural disasters. Collectively, the

15 scenarios are designed to focus contingency planning for homeland security preparedness work at all levels of government and with the private sector. The scenarios form the basis for coordinated federal planning, training, exercises, and grant investments needed to prepare for emergencies of all types.

“The Universal Task List” (UTL), which is a menu of some 1,600 unique tasks that can facilitate efforts to prevent, protect against, respond to, and recover from the major events that are represented by the “National Planning Scenarios”. It presents a common vocabulary and identifies key tasks that support development of essential capabilities among organizations at all levels. Of course, no entity will perform every task.

“The Target Capabilities List” (TCL) defines 37 specific capabilities that communities, the private sector, and all levels of government should collectively possess in order to respond effectively to disasters.

The desired end-state of the Preparedness System is to achieve and sustain coordinated capabilities to prevent, protect against, respond to, and recover from all hazards in a way that balances risk with resources. The Preparedness System provides opportunities for all levels of government, the private sector, nongovernmental organizations, and individual citizens to work together to achieve priorities and capabilities outlined in the “Guidelines”.

## **6. Chemical Security, Preparedness**

“The Chemical Countermeasures Thrust Area” develops technology to reduce vulnerability to chemical warfare agents (CWAs) and commonly used toxic industrial chemicals (TICs) and provides countermeasures to emerging non-traditional chemical threat agents (NTAs). “The 3 Main Program Areas” in the chemical countermeasures thrust area include the following: analysis, detection, and response recovery.

“Analysis Program” develops a robust and enduring analytical capability to support the chemical countermeasures development. Activities focus on developing a fundamental understanding of toxic chemical threat properties and conducting risk and vulnerability assessments based on these properties; developing and sustaining expert reach-back capabilities to provide rapid support in domestic emergencies; and developing and validating forensic methodologies and analytical tools, such as chemical signatures, which are used to help identify the nature and origin of chemical threats used by terrorists and criminals.

“Detection Program” develops technology to warn and notify of a chemical threat release. It includes technologies responders need to survey potentially contaminated scenes, while limiting their exposure to chemical agents. This program aims to provide technologies that can, in a single package, sense chemical agents and more commonly

monitored chemicals, at costs that will support dual-use application. Due to the various physical properties associated with detecting “high-vapor pressure versus low-vapor pressure chemical threats”, an array of technologies is required to ensure that the full spectrum of chemical hazards is adequately addressed.

“Response and Recovery Program” provides technologies for returning a chemically contaminated area to a normal condition. This work primarily supports the development of technologies and guidelines for decontamination and the analysis of contaminated areas both before and after restoration processes. These efforts will decrease the duration of cleanup efforts after an attack with a chemical agent on key infrastructure and include supporting capabilities such as the development and demonstration of facility restoration and decontamination technologies and guidelines; development of a “mobile chemical analysis laboratory”; and the development of “fixed-site chemical analysis laboratories” for CWAs.

## **7. Food-Bio-Security and Bio-Terrorism**

“The Chemical and Biological Division” has defined “6 Strategic Objectives” to help accomplish its mission. These are to enable comprehensive understanding and analyses of biological and chemical threats in the domestic domain; develop pre-event assessment, discovery, and interdiction capabilities for biological and chemical threats;

---

develop capability for warning, notification, and timely analysis of biological and chemical attacks; optimize technology and process for recovery from biological and chemical attacks; enhance the capability to identify biological and chemical attack sources; and develop vaccines and diagnostics for high-priority foreign animal diseases.

“The Biological Countermeasures Thrust Area” provides the understanding, technologies and systems needed to protect against possible biological attacks on population or infrastructure. The thrust area focuses primarily on those biological attacks that can potentially cause widespread catastrophic damage. Where appropriate, the program incorporates bio-defense as part of an integrated “chemical, biological, radiological, nuclear and explosive” (CBRNE) defense across civil and military agencies. “The 5 Main Program Areas” in the biological countermeasures thrust area includes: threat awareness program, surveillance and detection program, response and restoration program, and forensics program.

“Threat Awareness Program” characterizes threats posed by biological weapons, anticipates future threats, and conducts comprehensive threat and risk assessments to guide prioritization of the nation’s bio-defense investments. The primary deliverable is an intelligence-informed, scientific characterization and prioritization of bio-terrorist risks. This deliverable is used by OHA, the Homeland Security Council (HSC) and other agencies such as the Department

of Health and Human Services (DHHS), EPA, Department of Agriculture (USDA), and the Intelligence Community (IC) to support their efforts in enhancing the bio-defense.

“Surveillance and Detection Program” develops next-generation detectors for biological threat agents, including fully autonomous detection capabilities for the third generation (Gen 3) Bio-Watch system. In addition, this program works to develop the assays (i.e., signatures or fingerprints of biological agents) needed by detectors to accurately recognize a biological agent.

“Response and Restoration Program” provides advanced planning, develops concepts-of-operation, and funds exercises and training for responding to and recovering from a large-scale biological attack. The objective is to provide a more rapid and less expensive post-attack cleanup and restoration in such situations.

“Forensics Program” operates the National Bio-Forensics and Analysis Center (NBFAC) and conducts bio-forensics research in support of criminal investigative cases, with the ultimate goal of attribution, apprehension, and prosecution of the perpetrator to fulfill Bio-defense for the 21st Century. These activities provide facilities, analytical methods, and rigorous chain-of-custody controls needed to support the FBI and others in their investigation of potential bio-crimes or acts of bio-terrorism. Additional research and development projects in this program area work to develop

improved methods for extracting genetic materials and proteins from samples for biological, chemical, and physical characterization.

At this point, we need to mention “Bio-surveillance”. In 1999, the University of Pittsburgh’s Center for Biomedical Informatics deployed the first automated bioterrorism detection system, called RODS (Real-Time Outbreak Disease Surveillance). RODS is designed to draw collect data from many data sources and use them to perform signal detection, that is, to detect the possible bioterrorism event at the earliest possible moment. RODS, and other systems like it, collect data from sources including clinic data, laboratory data, and data from over-the-counter drug sales. In 2000, Michael Wagner, the co-director of the RODS laboratory, and Ron Aryel, a subcontractor, conceived of the idea of obtaining live data feeds from “non-traditional” (non-health-care) data sources. The RODS laboratory’s first efforts eventually led to the establishment of the National Retail Data Monitor, a system which collects data from 20,000 retail locations in the country. Its principles apply to both natural and man-made epidemics (bioterrorism).

### **8. Nuclear-Radiological Preparedness,**

“The Domestic Nuclear Detection Office” (DNDO) is a jointly staffed office established April 15, 2005 to improve the capability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological

material for use against the country, and to further enhance this capability over time. Strategic Objectives are; to develop the global nuclear detection and reporting architecture, develop, acquire, and support the domestic nuclear detection and reporting system, fully characterize detector system performance before deployment, establish situational awareness through information sharing and analysis, establish operation protocols to ensure detection leads to effective response, conduct a transformational research and development program and establish the “National Technical Nuclear Forensics Center” to provide planning, integration, and improvements to USG nuclear forensics capabilities.

“Domestic Nuclear Detection Office” has 2 main bodies. First is “Joint Analysis Center” (JAC) staffed with personnel from the “Departments of Defense”, “Energy”, “Homeland Security”, the “Federal Bureau of Investigation” and the “Nuclear Regulatory Commission”, the “Joint Analysis Center” (JAC) will provide status tracking for the United States Government Global Nuclear Detection Architecture. With a direct conduit from the alarm source to national assets for spectrum analysis, the Joint Analysis Center will provide 24/7 response for radiological alarm resolution and provide the capability to marry intelligence, illicit activity, and threats with a known radiological architecture that will provide total situational awareness to decision makers. The

---

JAC facilitates the USG Interagency Nuclear Decision Protocols to adjudicate nuclear detection events. The JAC achieves situational awareness through visibility into deployed components, access to information, and historical data. Information is received from deployed radiological/nuclear detection assets, radiological/nuclear related events, the global nuclear detection architecture, the NRC and Agreement State Material Licensing Data, and historical data on all detection events, illicit and legitimate.

Second is “Operations Support Directorate” (OSD). The Operations Support Directorate within the Domestic Nuclear Detection Office is responsible for; establishing and operating a real-time situational awareness and support capability by monitoring the status of, and collecting information from, both overseas and domestic detection systems through the Joint Analysis Center and other programs. Operational support services include the development of protocols and standards, as well as a technical support infrastructure, or reach back, to ensure appropriate expertise is in place to support prompt alarm resolution.

### **9. Information among Agencies**

“Intelligence Analytic Priorities” (I&A) seeks to optimize the capability to collect and analyze intelligence and information and produce finished analyses tailored to the needs of key customers. I&A provides the decision makers with a timely, actionable, and complete understanding of

homeland security threats to facilitate informed decision-making, policies, and appropriate operational responses.

I&A has 5 analytic thrusts, aligned with the principal threats to the homeland addressed by the Department. The first is threats related to border security. The second is the threat of radicalization and extremism. The third is threats from particular groups entering the country. The fourth is threats to the Homeland’s critical infrastructure and key resources (CIKR). The fifth is weapons of mass destruction and health threats.

“State and Local Fusion Centers” are the partners at state, local, and tribal governments and the private sector gathering information outside the boundaries of the IC. Simultaneously, their information needs are not always recognized by traditional IC agencies. To meet their own all-threats, all-hazards information needs, many states and larger cities have created fusion centers, which provide state and local officials with situational awareness. Fusion centers are the logical touch-points to access local information and expertise as well as provide with timely, relevant information and intelligence derived from all-source analysis. The result is a new intelligence discipline and tradecraft that gives a new, more complete understanding of the threat. The Department provides personnel and tools to the fusion centers to enable the “National Fusion Center Network”.

## 10. Laws in Homeland Security

There are two main concerns or focal points while preparing due legal proposals. First one is “Balancing crime control and due process” and the second one is “Balancing Homeland Security and National Security with due Process”. Any unbalanced procedure will lead to create a problem. “Balancing Process” provides Legislation and court decisions that guide government investigations, rights of citizens and non citizens, profiling, civilian courts and military justice. It also regulates more, such as; Chemical Security Laws, Border Security Laws and Regulations, Preparedness Recovery Laws & Regulations, Infrastructure Protection and Travel Procedures.

## 11. Cyber Security

The “National Strategy to Secure Cyberspace”, is a component of the larger “National Strategy for Homeland Security”. “The National Strategy to Secure Cyberspace” was drafted by the Department of Homeland Security in reaction to the September 11, 2001 terrorist attacks. Released on February 14, 2003, it offers suggestions, not mandates, to business, academic, and individual users of cyberspace to secure computer systems and networks. It was prepared after a year of research by businesses, universities, and government, and after five months of public comment. The plan advises a number of security practices as well as promotion of cyber security education.

“The National Strategy to Secure Cyberspace” identifies “3 strategic

objectives” are: prevent cyber attacks against critical infrastructures; reduce national vulnerability to cyber attacks; and minimize damage and recovery time from cyber attacks that do occur.

To meet these objectives, the National Strategy outlines “5 National Priorities”: The first priority is the creation of a “National Cyberspace Security Response System”, focuses on improving the government’s response to cyberspace security incidents and reducing the potential damage from such events. The second is the development of a “National Cyberspace Security Threat and Vulnerability Reduction Program” and the third is the creation of a “National Cyberspace Security Awareness and Training Program”. The fourth of priorities is the necessity of “Securing Governments’ Cyberspace” aiming to reduce threats from, and vulnerabilities to, cyber attacks. The fifth priority is the establishment of a system of “National Security and International Cyberspace Security Cooperation”, intends to prevent cyber attacks that could impact national security assets and to improve the international management of and response to such attacks.

Ultimately, the strategy encourages companies to regularly review their technology security plans, and individuals who use the internet to add firewalls and anti-virus software to their systems. It calls for a single federal center to help detect, monitor and analyze attacks, and for expanded cyber security research and improved government-industry cooperation.

---

## **12. The Media and Homeland Security**

As a “Public Information Overview”, media is a part of communication tool with public to send critical information. Via media all population will be informed about everything needed during a crisis situation. As a result of this concept; “Public Information” consists of the processes, procedures, and systems to communicate timely, accurate, and accessible information on the incident’s cause, size, and current situation to the public, responders, and additional stakeholders (both directly affected and indirectly affected). Public information needs to be coordinated and integrated across jurisdictions, agencies, and organizations; among Federal, State, tribal, and local governments; and with NGOs and the private sector.

Well-developed public information, education strategies, and communications plans help to ensure that, lifesaving measures, evacuation routes, threat and alert systems, and other public safety information are coordinated and communicated to numerous audiences in a timely, consistent manner.

In order to facilitate that process, Public Information includes “3 Major Systems/Components”; “The Joint Information System” (JIS), and this system includes “Joint Information Center” (JIC) and “Public Information Officers” (PIOs). A Joint Information Center (JIC) is a central location that facilitates operation of the Joint Information System. The JIC is a

location where personnel with public information responsibilities perform critical emergency information functions, crisis communications, and public affairs functions. JICs may be established at various levels of government or at incident sites, or can be components of “Multiagency Coordination Systems”. A single JIC location is preferable, but the system is flexible and adaptable enough to accommodate virtual or multiple JIC locations, as required.

## **13. Securing Critical Infrastructure**

From energy systems that power our neighborhoods, to transportation networks that move us around our communities and the country, to facilities that provide people with safe drinking water, “Critical Infrastructure and Key Resources” (CIKR) impacts nearly every aspect of our daily lives. In short, CIKR is an umbrella term referring to; the assets of country’s essential to the nation’s security, public health and safety, economic vitality, and way of life.

There are “18 Sub-sectors” under this title; Agriculture and Food Sector, Banking and Finance Sector, Chemical Sector, Commercial Facilities Sector, Communications Sector, Critical Manufacturing Sector, Dams Sector, Defense Industrial Base Sector, Emergency Services Sector, Energy Sector, Government Facilities Sector, Healthcare and Public Health Sector, Information Technology Sector, National Monuments and Icons Sector, Nuclear Reactors, Materials, and Waste Sector, Postal and Shipping

Sector, Transportation Systems Sector and Water Sector.

There are a lot of programs and resources that foster public-private partnerships, enhance protective programs, and build resiliency to withstand natural disasters and terrorist threats. “Key Activities” in those areas include: assessing vulnerabilities, implementing protective programs, and improving security protocols, enhancing preparedness through training and exercises, assisting with contingency planning, response, and recovery, implementing real-time information sharing, implementing cyber security measures, assisting with infrastructure data collection and management, implementing regulations for high-risk chemical facilities and developing standards for federal building security.

Attacks on CIKR could significantly disrupt the functioning of country and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Attacks using components of the CIKR as weapons of mass destruction could have even more devastating physical and psychological consequences.

### **Conclusion**

The strategy for “Homeland Security” guides, organizes, and

unifies homeland security efforts. “Homeland Security” is a responsibility shared across and the strategy provides a common framework for the following four goals: Prevent and disrupt terrorist attacks; protect people, critical infrastructure, and key resources; respond to and recover from incidents that do occur; and continue to strengthen the system to ensure long-term success.

This updated Strategy, which builds directly from the first “National Strategy for Homeland Security” issued in July 2002, reflects increased understanding of the terrorist threats confronting the United States today, incorporates lessons learned from exercises and real-world catastrophes – including Hurricane Katrina – and proposes new initiatives and approaches that will enable to achieve “Homeland Security” objectives.

Today, “The Department of Homeland Security” has a mission, to secure the country from threats more than 225,000 employees in jobs that range from aviation and border security to emergency response, from cyber security analyst to chemical facility inspector. Protecting the people from terrorist threats is founding principle and highest priority. This is an effort where everyone - families and communities, first responders, the private sector, state and local governments has an important role to play. Every resource available toward prevention and preparedness, and empower people to live in a constant state of readiness, not a constant state of fear.

---

---

**Bibliography**

Bullock, Jane A., George D. Haddow, Damon Cappola, Erdem Ergin, Lissa Westerman and Sarp Yeletaysi, *Introduction to Homeland Security*, Elsevier, Butterworth, Heinemann, Massachusetts, MA, Oxford , 2006.

Forest, James, Joanne Moore and Russel Howard, *Homeland Security and Terrorism: Readings and Interpretations*, Mc Graw Hill, New York, NY, 2006.

Purpura, Philip P., *Terrorism and Homeland Security: An Introduction with Applications*, Elsevier, Butterworth, Heinemann, Massachusetts, MA, Oxford, 2007.

Sauter, Mark A. and James Jay Carafano, *Homeland Security: A Complete Guide to Understanding, Preventing and Surviving Terrorism*, Mc Graw Hill, New York, NY, 2005.

US Department of Homeland Security, <http://www.dhs.gov>.

---

## Defence Against Terrorism

**Fevzi Birkal ÇUHADAR\***  
**Maj. Tamer SERT\*\***

### 1. General Information

 COE-DAT conducted a course on Defence Against Terrorism on 10-14 May 2010 in Ankara/Turkey. The aim of this course was to enable effective support to NATO, Partnership for Peace (PfP), Mediterranean Dialogue (MD), Istanbul Initiative Countries (ICI) and other nations' personnel together with 47 Iraqi trainees since they are involved in planning DAT policy and operations. This course intended to assist staff officers in the development of policies and dealing with DAT issues and also devoted to staff and planners at the strategic and operational level. The course focused on the following objectives:

- a. To examine the causes of terrorism as well as its present and future characteristics,
- b. To be aware of the role of NATO in defence against terrorism (DAT),
- c. Overview on crisis management related to a terrorist attacks,
- d. To study terrorism and the media relations,
- e. To study general threat assessment of cyber terrorism,
- f. Terrorism and intelligence,
- g. To understand the importance of the threat of Weapons of Mass Destruction (WMDs).
- h. Working groups and their presentations.

The content of the lectures and the conclusions had drawn from this course display will be published in the book format in late 2010. The course was funded by COE-DAT shared budget.

This course added an important dimension to the Centre's work on counter-terrorism. COE-DAT was able to bring contemporary practical knowledge and academic expertise, including the long experience built up by Turkey on DAT, and a participatory audience from the NATO Countries, to bear on defence against terrorism.

The Centre was seeking to reach a common understanding of the framework of DAT expertise and input to future policy development.

According to the final roster, there were 98 participants, 74 military and 18 non-military personnel, 27 from NATO, 9 from PfP, 2 from MD, 2 from ICI, and 52 from other nations in the course.

Each panel contained 4-5 presentations that lasted 45-60 minutes including the question and answers period. The last period of the course was composed of presentations by the 3 working groups composed of the course participants.

COE-DAT did receive an administrative assistance from NATO Training Mission Iraq (NTM-I) to a certain degree for the participation of Iraqi delegation, which was composed of 47 Iraqi personnel. United Nations (UN) Counter-Terrorism Executive

\* (TUR POL), 1st Grade Chief of Police, COE-DAT Course Director.

\*\* (TUR A), COE-DAT Course Director.

Directorate (CTED) and US Military Academy (West Point) supported the course with Subject Matter Experts (SME). In total, there were 16 lectures by 12 instructors, one case study and three working group presentations on the topics of history and causes of terrorism; terrorism, security and democracy; legal aspects of DAT; organized crime and terrorism; theology and question of violence in religion; terrorist recruitment; financing terrorism; WMD terrorism; cyber terrorism threat assessment; media and terrorism; NATO DAT policy, structure and MC 472; strategic communication in terrorism; crisis management and terrorism; homeland security in combating terrorism; the role of intelligence in combating terrorism; NATO's role in combating against terrorism and a case study by an Iraqi expert based on his own experiences and opinions.

There were also social events included in the course programme such as the icebreaker cocktail on 10 May 2010, at Merkez Officers Club; an Official reception on 12 May 2010, at NCO Club (hosted by Director, COE-DAT) and a Cultural tour in Ankara on 13 May 2010.

## 2. Conclusions

Independent scholars, consultants and military personnel provided the participants with lectures about different dimensions of terrorism. The question and answers period together with the working group activities resulted in fruitful discussions.

### a. Assoc. Prof. Salih BIÇAKÇI<sup>1</sup>

The lecture by Assoc. Prof. Salih BIÇAKÇI was on "Terrorism, Security and Democracy". The premise of his speech was the relationship between democracy and terrorism, which sometimes turn out to be a dilemma. He highlighted reactions towards terrorism, counterterrorism, promotion of democracy, national security and the importance of cooperation in countering terrorism.

He emphasized that democratic governments have a responsibility to educate their publics and to encourage heightened democratic solidarity, not fear, in the face of terrorism. According to him, governments should not rush into decisions that are based on public pressures due to fear or hatred. Rather, the response must be considered, deliberate, and controlled by the civilian authorities. He also discussed that democracy is not an output but a process.

He later put forward that security is generally perceived as "national security" rather than international security. Thus, national security is subjective and not compatible with international security. In the end, he emphasized again that cooperation at the international level requires cultural awareness, building up trust and understanding various ways of communication.

### b. Maj. Julian CHARVAT<sup>2</sup>

The first lecture by Major Julian CHARVAT was about "NATO DAT

<sup>1</sup> Professor at the International Relations Department of Işık University.

<sup>2</sup> (UK A), Course Director in COE-DAT.

Policy, Structure and MC 472". He highlighted that the fight against terrorism is a permanent agenda item and priority for the Alliance. In combating terrorism, NATO helps to ensure that individuals can continue their daily lives safely, free from the threat of indiscriminate acts of terror.

The Alliance offers a unique range of assets to the international community in the fight against terrorism. First, it is a permanent consultation forum, which can transform discussions into collective decisions. Second, this is backed by unparalleled military capability at the Alliance's disposal. Third, NATO is part of an impressive network of cooperative relations with many partners.

Since the fight against terrorism has been identified as a core element of the Alliance's work, NATO has established regular dialogue on terrorism and terrorism-related issues among its members, as well as with non-member countries and other international organizations.

Maj. Julian CHARVAT also indicated that NATO is developing capabilities and innovative technology that specifically address the issue of terrorism. The aim is to protect troops, civilians and critical infrastructure against attacks perpetrated by terrorists, such as suicide attacks with improvised explosive devices, rocket attacks against aircraft and helicopters, and the potential use of weapons of mass destruction.

Furthermore, he underlined the United Nations Security Council Resolution (UNSCR) 1368 which was adopted on 12 September 2001 and Article 5 of the Washington Treaty which was invoked first time in NATO's history after 9/11. In addition, he emphasized that although state sponsorship of terrorism is currently in decline, political circumstances could lead to its rise, such as providing terrorists with safe havens and considerable resources. He went on by stating that timely and accurate intelligence is an essential requirement in successful deterring and protecting against terrorist attacks. Finally, NATO forces could provide assistance to a nation wishing to withdraw its citizens or forces from an area of increased terrorist threat. The threat is severe enough to justify acting against these terrorists and those who harbour them, as and where required, as decided by the North Atlantic Council (NAC). As the Alliance has refined its counter-terrorism role, the operation's mandate has been regularly reviewed and its remit extended.



The second lecture by Maj. Julian CHARVAT was on “Cyber Terrorism”. He began with the idea that there have been many attempts to define terrorism at the international level which have not been successful due to the lack of consensus. There are many factors to debate such as the cause, the victim, the activity and when exactly something crosses from political protest to terrorism. Many argue that terrorism cannot be against military targets while others demand a certain type of attack. The motivation is important in understanding why terrorism happens and, therefore, vital in solving the issue and bringing an end to it. It will also determine how far the terrorist will go and who are likely to be targets.

He emphasized that there is no actual definition of terrorism and thus, it is not surprising that Cyber Terrorism is widely debated. He briefly looked at how the terrorists are using the Internet in their campaigns. The Internet provides a great forum to share information. It is also an unregulated space and therefore, anyone can put up information about anything.

He went on by stating that terrorism does not have to be expensive but to achieve major attacks some financing is needed. There is a debate about cyber terrorism. Can it happen? Why has it not happened? Does not terrorism have to break things or kill people? One of the difficulties of cyber terrorism is that it may not do any damage or we may not notice the damage. The terrorist has a multitude of possibilities

where they actually aggressively attack targeted cyber space. Terrorists are generally good at propaganda and as they are not bound by the truth or reality as we are, they have a great scope to exploit the use of the Internet for terrorist purposes. Terrorists have a message, which comes from their motivation, which they want to share with the world. Video sharing is a popular way for them to do this.

Generally, terrorist attacks break things down or kill people. But with cyber attacks this is hard to quantify. He stated that certainly terrorists use the Internet for command and control, recruiting and financing their activities, but if this is cyber terrorism is a matter of debate. Many would say that it is not since it is traditional terrorist activities using a new medium, the Internet. Finally, he emphasized that the defence against cyber terrorism are the same as the ones for any cyber security issue. Good back up, alternative servers and spare bandwidth all help. Also careful use of security measures is essential.

### **c. Assoc. Prof. Mustafa KİBAROĞLU<sup>3</sup>**

Assoc. Prof. Mustafa KİBAROĞLU gave a lecture on “Defence Against WMD Terrorism”. He elaborated on, the nature of the threat, countermeasures as well as cyber threat. He identified Nuclear Weapons as the explosive devices that release huge amounts of energy and radiation achieved by splitting the fissile material (HEU and/or Plutonium) resulting in a

self-sustained chain reaction. He underlined Chemical Weapons as toxic chemical substances that cause incapacitation, injury, or death of the target population (humans, animals, and plants) and Biological Weapons, as infectious diseases that cause incapacitation or death of the target population (humans, animals, and plants).

Non-state actors (i.e., terrorist organizations) do usually declare their intentions in order to disseminate fear and/or to make propaganda and advancements in science and technology to help terrorist organizations develop and/or acquire advanced weapons capabilities including WMDs. Terrorist organizations do not need sophisticated weapons systems. “Crude” or “dirty” weapons will suffice for terrorists to achieve their goal.

Means and methods of attack may require simple machinery or techniques. Dispersing a chemical and/or a biological agent can be carried out by agricultural sprayers, ventilators, or a civilian aircraft. Industrial facilities, critical infrastructure, harbours, airports may be primary targets. One way to eliminate the possibility of terrorism with WMD would be to eliminate the availability of all nuclear, chemical, biological and radiological material that can pass into the hands of terrorist groups. But, this is not possible due to the existence of WMD stockpiles in a number of states, material coming from dismantlement of weapons, nuclear power and research reactors, dual-use chemical and biological facilities, nuclear, chemical, biological research laboratories.

#### **d. Prof. Dr. Şaban Ali DÜZGÜN<sup>4</sup>**

Prof. Dr. Şaban Ali DÜZGÜN presented two lectures, one on “Theology and Question of Violence in Religion”; and the other on “Winning Back Religion: Countering The Misuse of Scripture Against Terrorism”. During his presentation, Prof. DÜZGÜN mainly focused on Islam of identity and Islam of truth; subordination scripture to the politics: the position of Islamists and ‘ulamā in contemporary Islam; para-mosque structures and transformation Islam into Islamism; neo-Orientalism, essentialism and contingencies about scripture and its relation to Muslims’ behaviour; jihad and associate terms; suicide bombings and their (un)justification.

Without referring to the scripture, it is hardly reasonable to explain the mind and the actions or phenomena created by this mind. But it is also not realistic to explain the mind and actions referring completely to the scripture. As the text is just one of the components that produces this mind and actions beside cultural and geographical milieu, to get an authentic evaluation all these factors have to be scrutinized together. We must admit that Islam could have more than one interpretation. Muslims in different geographies are not pure products of their religion. If so the best Muslim could not be other than Muslim extremist who claim the literal structure of scripture.

He went on stating that exclusionary and repressive political environments in their

<sup>4</sup> Professor at the Theology Department of Ankara University, Turkey.

home country force Islamist to undergo a near universal process of radicalization, which has been witnessed by so many rebellious movements. But why they transform Islam into a means of rebellion is something else to be questioned. Prof. DÜZGÜN also mentioned the term jihad which evokes differing sentiments. For some observers, it conveys the idea of the fanatical Arab horseman, galloping wildly into battle with unsheathed sword flashing in the sun, offering men and women the choice of accepting Muslim religious traditions or death. So, what does jihad mean today? Why are all these terrorists taking their lives and killing innocent people in the name of Islam? Why are they conducting their jihad? It is unfortunate that today with regard to jihad, mostly political analysts take the podium. One reason why some Muslims have associated jihad with violence, while the great majority reject this is its being part of any political jargon. He also mentioned the suicide bombers who are striking the

Western and non-Western cities use a religious language, affirm religious identities and see the world through specific religious interpretation. As a matter of fact, Islamists mostly do not support suicide bombings.

Finally, he emphasized that Muslim leaders must continue to speak against violence, brutality, and injustice, as they reject terrorism and indiscriminate violence against civilians and demand that the Islamic respect for the sanctity of human life, and the Islamic injunction against the killing of innocents be strictly observed. But this is not enough. Muslim leaders must go beyond the condemnation of terrorism to become more active in exposing the roots of violence, hatred, and terrorism.

**e. Assoc. Prof. Dean  
ALEXANDER<sup>5</sup>**

Prof. ALEXANDER gave a presentation on “Law Enforcement Responses to Terrorism”. He outlined international legal responses to terrorism, regional legal responses to terrorism, national legal responses to terrorism: United States, lessons learned and what challenges remain? He put forward effective counterterrorism legal strategies. Some of these are crafting clear policy and mission statements, designing strategies to support the policy, reorganizing prosecution teams into specialized units and increasing international cooperation.

He stated that terrorism is the threat and/or use of violence for a ‘political’ objective undertaken by individuals, groups, and countries



<sup>5</sup> Director Homeland Security Research Program and Associate Professor in Western Illinois University, Macomb, Illinois, USA.

against non-combatants in violation of law. Terrorist groups (TG) are organizations composed of multiple individuals who contribute to the undertaking of terrorist activities. Self-selected terrorists, without any connection with others or a group, are excluded. Terrorism, whether undertaken domestically or internationally, can have monumental effects on all aspects of daily life: security, safety, socio-economic aspects, etc. Organized criminal syndicates (OCS) are structured groups of three or more persons, existing for a period of time and acting in concert with the goal of committing serious crimes in order to obtain financial or material gain. [UN Convention Against Transnational Organized Crime] OCS are involved in illegal activities ranging from drug trafficking, illegal immigration and trafficking in human beings, money laundering to fraud.

He has also compared Terrorist Groups and Organized Crime Syndicates:

1. At their core, TG have ideological goals which are served through the use of violence. Economic interests are relevant as they provide resources to the TG. Yet some groups have convergence in these realms.
2. Money, not ideology, is the principal driver of OCS activities. Violence is utilized to ensure the money flow.
3. Both operate globally, thrive in unstable environs with weak laws and governments.
4. Both use legal businesses to undertake traditional transactions

(e.g., purchase computers, airline tickets, bank accounts, phone, mail couriers, Internet services) that advance their criminal interests. Likewise, they may establish front companies that are used to purchase weapons and mask ownership.

5. Both enter into relationships with illicit entities in order to obtain forged documents, weapons, and drugs.

#### **f. Dr. Nicholas RIDLEY<sup>6</sup>**

Dr. RIDLEY presented on the financing of terrorism and the role of intelligence in combating terrorism. According to him, terrorism and organised crime are intermingling so that 'convergence of causes' renders terrorism indistinguishable.

He went on with an example about IRA. He later mentioned money laundering, terrorist financing, fund raising and illicit transferring. 1994 United Nations General Assembly passed Resolution 49/60, approved a Declaration to Eliminate International Terrorism, against the role of states or countries supporting certain types of terrorism. It was followed by UN Resolutions 51/201 of 1997 and 531/80 1999. Before 9/11, only four of the 22 ratifications needed to bring this into force had been deposited with the UN Secretary General.

Furthermore, he elaborated the disadvantages of international anti-terrorist legislation. He emphasized the issue of time lag since all countries have to agree about the legislation as well as the issue of who terrorists are since

domestic implications to and every individual country is different. He also stressed the possible negative factors in anti-terrorist legislation such as timing, principle of something must be done immediately, duplication (passing new legislation where such powers already exist), unreal objectives, excessive powers, indirect application (use of new legislation for other criminal offence purposes).

**g. Col. M. Uğur ERSEN<sup>7</sup>**

Col. ERSEN presented the issue of “Terrorist Recruitment”. He started with by asking: the question of why terrorist organizations need recruitment. Geographical reach, high turnover rate (losses), policy (limited experienced member), flexibility to change direction are counted as the reasons. Then he continued with the question of how being a terrorist become attractive There are some answers to this question like Maslow’s theory in terms of adherence to values, imaginary scenario - trap, ethnic, social, religious, psychological framing, terrorist versus hero, triggering events, and root causes. He also listed characteristics of recruits as mentally normal, middle class , having middle to high education, unemployed or temporary worker, single or having no child, having family problems and younger than the age of 30.

Some specific reasons to join the terrorist organization are identified as being out of boredom, desiring to have an action packed adventure, being a well-known, but mysterious figure, using their

special skills, occasional protest and opposition, personal experiences of victimization, violent actions by security forces and personal expectations.

He also put forward some survey results through candidate-information collection and new trends by mentioning post-recruitment process. Finally, he emphasized that psychological treatment, countering-ideological rehabilitation, continuous observation are important counter-recruitment measures.

**h. Col. Özden ÇELİK<sup>8</sup>**

Col. ÇELİK delivered a presentation on “History and Causes of Terrorism”. By stating that terrorism is not a new phenomenon, and has a long history, he explained that modern terrorism has similar characteristics with the earlier forms of terrorism. Today’s terrorists are using almost the same tools, motives, events, inspiration and theoretical arguments that were also popular in much earlier eras.

He elaborated the history of terrorism within pre-modern and modern periods. He stressed the assassination of Julius Caesar, Sicariis in Judea, Hashashshins and Thugs of India as the examples of terrorism in the pre-modern period. He examined terrorism in the modern period under four waves: 1890-1920, 1920-1970, 1970-1980 and 1980 up to now. Within this categorization, he stressed that with the 1960s, terrorism has attracted international attention and gained an international scope.

With respect to the causes of terrorism, he underlined that

<sup>7</sup> (TUR AF), COE-DAT Course Director.

<sup>8</sup> (TUR A), COE-DAT Acting Chief of Education and Training.

terrorism can be seen everywhere, in every nation and society regardless of level of development, political system and demographic structure. He also stressed that terrorists can be found among normal or abnormal, educated or uneducated people. Therefore, it is hard to make any generalization about the causes of terrorism or the characteristics of terrorist. In this context, he analyzed the causes of terrorism under four categories: contextual causes (globalization, deprivation and poverty), convictional causes (political causes, ideological causes, religious factors and subordinate convictions), motivational causes (psychological, cultural, rational causes, social movements, dramatic events, immediate circumstances), facilitating causes (developments in technology, transportation, communication, news media, state sponsorship, weak states.). He concluded that terrorism may originate from many sources and thus, social, economic, political, religious conditions and philosophy existing should be scrutinized at particular time and place.

#### **i. Maj. Aykut ÖNCÜ<sup>9</sup>**

Maj. ÖNCÜ lectured on “Strategic Communications in Combating Terrorism”. He defined strategic communications as massing of information and actions to influence attitudes and behaviour of target audiences. Strategic Communications should be gone with the synchronized promulgation of information, ideas and actions over time through means and content that are tailored for multiple and diverse audiences.

Strategic Communications intend to use behavioural change as a leverage on target community to reach objectives, innovate and adapt effort across all arms of government to achieve expected effort at the right time, place and target, coordinate and harmonize all related activities leading to objectives. Maj ÖNCÜ underlined that messages can persuade when they agree with actions and consistent. They are interpreted on the basis of our mental filters, emotions and interpretations of the sender’s intentions.

He concludes that “Strategic Communications” must be regarded as fundamental element for all efforts in combating terrorism. Mutual understanding and listening will help us to understand real causes of problems and show the way for how to solve them.

#### **j. Ms. Zeynep SÜTALAN<sup>10</sup>**

Under the heading of “NATO’s role in Combating Terrorism”, Ms. SUTALAN spoke about NATO’s approach to terrorism so far and the conceptual debates that are taking place in NATO, about the future security challenges, one of which is terrorism. She explained that with the end of Cold War, international security environment has changed a lot. Risks and threats to international security multiplied and have become more multi-dimensional as the borders with the national, transnational, international and global blurred. The complexity of the threats enforced a change in the comprehension of the security environment and the requirements

<sup>9</sup> (TUR A), COE-DAT Concept Officer.

<sup>10</sup> Civilian, PhD Candidate, COE-DAT Concept Specialist.

to deal with the new threats, new, not in the sense that they did not exist before, but new, in the sense that their nature has changed. Such changes had an impact on NATO's approach and transformation which are reflected in the strategic concepts of 1991 and 1999.

Within this framework, she touched upon how terrorism as a security challenge is reflected in NATO's strategic concepts, summits as well as concepts. She also elaborated the Multiple Futures Project and its implications on NATO's policy and concepts. As one of the most significant findings of the Multiple Futures Project, she underlined was the anticipation that the environment will include conventional, irregular, terrorist and criminal elements in mixed modes of operations.

She concluded that the growing complexity of the threats as indicated in the discussions on hybrid threats may necessitate the development of the new capabilities or adapting the present ones. In this respect, NATO will continue its determination in the fight against terrorism as well as its transformation as a dynamic body trying to adapt itself to the conditions of the security environment.

#### **k. Maj. Kenan TOKGÖZ<sup>11</sup>**

Maj. TOKGÖZ delivered a lecture on "Terrorism and Media". According to NATO, "terrorism is the unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to

achieve political, religious or ideological objective."

Since terrorism is a global threat, combating terrorism also requires global cooperation. The absence of a clear and common definition is the sign of absence of mutual cooperation and understanding in international community. At past, some countries thought that they're immune from terrorism threat or some of them thought if they don't mess with terrorists, they will not give harm to them. But today we see that no country is immune from this threat and you can't get rid of terrorism by ignoring it. Nations have been condemning or complaining terrorism with the harshest available terminology when they themselves suffer from it, but otherwise they prefer to turn a blind eye to the sufferings of other nations.

For example, The PKK/KONGRA-GEL terrorist organization, which is responsible from the deaths of thousands of Turkish citizens including not only the soldiers and police officers but also civilian people, women and children and even babies, is in the list of Terrorist Organizations of both the EU and the US. But when we look at the certain media channels in these countries, they still present the PKK/KONGRA-GEL terrorist organisation as a guerrilla group or insurgents. The reality that "one man's terrorist is another man's freedom fighter" is the fundamental reason for the absence of international cooperation. Sincerity in the cooperation against terrorism is the key to success in this fight.

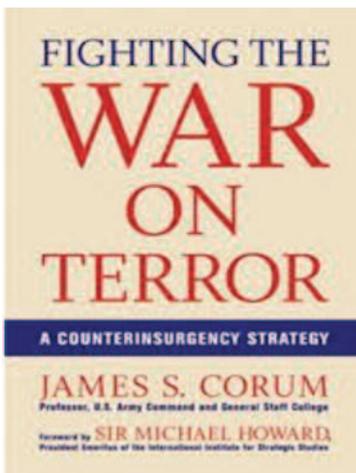
<sup>11</sup> (TUR A), MET Officer.

## Book Review

Maj. Aykut ÖNCÜ\*

### **Fighting the War on Terror: A Counterinsurgency Strategy,**

James S. Corum. St Paul, MN: Zenith Press, 2007, 304 p. ISBN-13: 978-0-7603-2868-2



The author, James S. CORUM, finds the United States (US) counterinsurgency (COIN) campaign unsuccessful. He focuses on the basic reasons of this failure and recommends solutions for success. Contrary to some influential US military staff officers the author has recently encountered, he believes that the US and its allies can defeat insurgencies, although it will be a very long and challenging process. The author asserts that the success requires some reforms and changes both in military and civilian sides of the US administration.

CORUM emphasizes the importance of understanding the nature of the conflict and criticizes that this is a major problem for the time being. In the aftermath of Vietnam and Cold War era, he argues that there have been changes in the motivation for insurgency. The main factors to motivate the people to join an insurgent organization are ideology, nationalism, ethnic nationalism and religion although some officials can not understand that in reality most past insurgencies were motivated by ideology, nationalism, or a combination of the two. However, the primary motivations changed with the general rise of disorder in the world and the collapse of the bipolar political system. Since 1990, ethnic nationalism and religion have been the main motivators for the insurgencies. These trends of combined ethnic and religious motivations for insurgents make counterinsurgency more difficult.

The view of the author is that the insurgency in Iraq is an example of

an insurgency organized into loose groups and networks, which complicates identification of organizational leadership by security forces. However, the US Army in Iraq still expects insurgency to follow a Maoist model of organization, a centrally led insurgent force operating under a unified insurgent command. The success or failure of the US efforts to fight insurgencies motivated by radical Islam will depend largely on how well military leaders can adapt their thinking to the new environment.

CORUM makes it clear that any counterinsurgency strategy must first understand the motivation for the insurgency and then deal with it. In this case, a broad push to support a more moderate approach to Islam and the more moderate Islamic states would be in order as a central element in counterinsurgency strategy. Thus, military leaders must adapt the military forces to fight insurgency and terrorism and change their well-established conventional war doctrine.

The author lays out a thought that America's "New Way of War" was far from the realities of today's world. He asserts that the Gulf War in 1991 made a common belief among the high-rank officials that technology had become the single most decisive aspect of warfare and developed a revolutionary answer to modern warfare and that old wisdoms about war should simply be discarded. The Bosnia campaign in 1995 and Kosovo in 1999 were presented publicly as the airpower alone won the war and glued this New Way of War in the minds. In

\* (TURA), COE-DAT Concept Officer.

addition, impermanent success of the US air campaign in support of the Afghan Northern Alliance forces in late 2001 contributed to this approach that New Way of War could be used in the war on terror as well. This new trend has caused a decrease in the number of Army and Marine troops which are the main tools in Global War on Terrorism (GWOT).

The current strength of deployed US forces in the COIN in rotation is inadequate to support the requirements of theater operations. On the other hand, there is a dilemma that the force strength requirements for Counter-Terrorism (CT) operations will compete with the requirement to equip and train the same forces for conventional war. Thus, the cost-effective solution is to give the conventional forces extra training for CT and use them in relatively safe areas. High risk missions must be conducted by Special Forces (SF) troops.

CORUM believes that “controlling populations” is the most important part of the War on Terror, and controlling the population is much more than just a police operation to maintain order, which also includes a large political element as well as social and economic elements. He argues that the mistakes in Iraq, in terms of controlling population, include miscalculations of US Military and Civil Affairs force strength that resulted from short sighted Pentagon policy which underestimated the role of these troops and minimized their peacekeeping role. Additionally, poor interagency cooperation has been a consistent problem with US nation-building

and counterinsurgency operations for decades. Control over the population is the goal of both sides in the campaign, insurgents and counterinsurgents. The failure of one side means the success of the other side in CT. Thus, interagency cooperation within the US government must be improved without establishing new layers in the bureaucracy.

Intelligence is assessed by CORUM to be another part that needs to be developed. He asserts that although the current impressive tactical and operational intelligence system built primarily around air reconnaissance, unmanned aerial vehicles (UAV) and space surveillance systems are very effective in conventional wars but shouldn't be applied to war against the insurgents so efficiently. He considers that the lack of effective Human Intelligence (HUMINT) is the biggest potential threat that can cause the US to fail in GWOT. He strictly recommends improving the HUMINT capability as soon as possible, being aware that it takes years to build an effective HUMINT infrastructure, including the linguists, modified to use in counterinsurgency even if the work starts now.

It is impossible not to agree with CORUM that in urban based insurgencies tightened HUMINT networks are desirable, but in rural areas the insurgents' mobility may limit HUMINT effectiveness. Signal Intelligence (SIGINT), including the UAVs, is still a very useful tool in CT Intel efforts. Thus, a balance established to the requirements of the battlefield and enemy must be kept.

The winning of hearts and minds, mostly the same center of gravity of all sides in the war, CORUM believes is obligatory in counterinsurgency. The media is the main tool to win the public support and to establish control in an occupied country or suppress an insurgency. CORUM states that the failure to build a democratic mass media plan for the early stages of Iraq was one of the grievous mistakes of the American military leaders and policymakers. His argument, that “for success in GWOT the US has so far to go in putting together a coherent and comprehensive message that will appeal to the average citizens of the Islamic states, who are bombarded daily with anti-western and anti-American messages” is the most striking point in the book.

Training local forces is important in counterinsurgency, CORUM stresses. It is a fact that not even a great nation with enormous military and economic power can hope to defeat a modern insurgency in another nation, or even keep any semblance of order for an extended period, without the active support of an effective indigenous security force. The US couldn't use the Iraqi troops effectively. Similarly in the past, the US could use effectively the trained local forces neither in Vietnam nor in Korea and had to use its own troops. If you have enough troops, it is the best and most effective way of command and control; however no state has enough manpower to fight insurgency overseas.

The book is most persuasive when CORUM presents the

recommendations for the success in GWOT as follows:

The US possesses adequate resources to fight insurgency; the point is how to allocate the nation's manpower and technical resources for warfare. The prevailing strategy of “do more with less” can lead to strategic defeat and a shortage of manpower for the American ground forces, could actually break the force, and America could soon end up with a worn-out army with low morale' low efficiency' and declining standards of competence.

The current US military education and training system is inadequate for the requirements for the GWOT, thus needs reform.

Alliances are necessary for victory and some allies require aide to reform, train and equip their security forces. Thus, the current military aid budget of which the 78 percent goes to Israel and Egypt must be rearranged to meet this requirement.

“Fighting the War on Terror: A Counterinsurgency Strategy” is a book that analyzes COIN, CT and the musts for success. This book does provide insight into the problems of US in Counterinsurgency generally and shows that there is actually nothing fundamentally new in conducting an effective counterinsurgency campaign. Insurgencies cannot be defeated via the rapid, decisive campaigns favored by American doctrine, thus the only need is to use the basic principles of effective counterinsurgency which are already known, however, surprisingly not used effectively by many military.

---

## COE-DAT ACTIVITIES

---



**1** COE-DAT conducted its **4th course** on “Cyber Terrorism” on 12-16 April 2010 in Ankara/Turkey. The issues of information security in NATO, cyber attacks against NATO, legal aspects of cyber terrorism, terrorist use of internet and cyber terrorism, terrorist communication in the cyber space, hacker profiling initiative, anonymity in the Internet, international cooperation in counter cyber terrorism and the protection of critical infrastructure, the role of intelligence in countering cyber terrorist operations, countering terrorist communication in cyber space. SCADA and national critical infrastructures security and organizing operational information assurance and computer network defence capability were discussed throughout the course. 61 participants from 28 different countries and 9 speakers from 5 different countries attended the course.

**2** The Commander of the Armed Forces of New Zealand, LTG Jerry MATEPARAE visited COE-DAT on 22 April 2010.





**3** COE-DAT carried out its **7th course** on “Defence Against Suicide Bombing” on 26-30 April 2010 in Ankara/Turkey. The course has been designed to elaborate the issue of suicide terrorism and how to defence against it. Accordingly, the conceptualization and history of suicide terrorism, suicide terrorism and media approach, root causes and motivation of suicide terrorism, demographic profile of suicide bombers, terrorist recruitment in suicide terrorism, suicide attacks outside the scope terrorism and the case of Kamikazes, modus operandi of suicide bombers, theology and question of violence in religion, religious justifications for suicide attacks, rules of engagement for suicide attacks, Turkish experience with suicide terrorism, the case of Pakistan in defence against suicide bombing, security measures for preventing suicide attacks and socio-political measures for preventing terrorism were elaborated during the course. 83 participants from 15 different countries and 11 lecturers from 5 different countries attended the course.

**4**

Chief of Operations of Hungary Army, MG Istvan JUHASZ, visited COE-DAT on 27 April 2010.



5

A delegation from the Hungarian Military Academy visited COE-DAT on 07 May 2010.



6

COE-DAT conducted a course on “Defence Against Terrorism” on 10-14 May 2010 in Ankara/Turkey. History and causes of terrorism, the relationship among terrorism, security and democracy, legal aspects of terrorism, NATO DAT policy and structure, NATO’s role in combating terrorism, WMD terrorism, cyber terrorism threat assessment, theology and the question of violence in religion, terrorism financing, organized crime and terrorism, media and terrorism, terrorist recruitment, crisis management and terrorism, the role of intelligence in combating terrorism, strategic communication in combating terrorism, Iraqi expertise on counter-terrorism, terrorism and law enforcement responses were analyzed during the course. 94 participants from 21 different countries and 12 speakers from 4 different countries attended the course.



7

COE-DAT conducted the **Advanced Training Course** on “Defence Against Terrorism: Different Dimensions and Trends of Emerging Threat; Terrorism” on 23-27 May 2010 in Kabul/Afghanistan. Throughout the course, the history and causes of terrorism, terrorism and civil disorder, legal aspects of fighting against terrorism, NATO DAT policy, structure and MC 472, homeland security in DAT concept, crises management and terrorism, legal aspects of military operations against terrorism, terrorism financing, terrorist recruitment and the role of intelligence in defence against terrorism, strategic communications, public relations and information management, organized crime and Asia and financing terrorism, the threat of WMD terrorism and future trends in terrorism were discussed. 37 participants from Afghanistan and 9 speakers from 4 different countries attended the course.

8

A delegation from Denmark visited COE-DAT on 18 May 2010.





9 COE-DAT carried out the **course** on “Efficient Crisis Management to Mitigate the Effects of Terrorist Activity” on 31 May-04 June 2010 in Ankara/Turkey. During the course, terrorism as a type of crime, internal crisis communication and information management, civil disorder management, interagency policy and strategy development, interagency planning and execution, roles and reactions of first responders, terrorism threat management, terrorism threat management, leadership in times of crisis, rules of engagement in a crisis situation, cyber threats as a future crisis, NATO crisis management, NATO and terrorism were analyzed. 25 participants from 14 different countries and 10 lecturers from 4 different countries attended the course.



10

MG Azhar Ali SHAN from Pakistan Army visited COE-DAT on 04 June 2010.



11

The Minister of Defense of Republic of Mali, Mr. Natié PLEA visited COE-DAT on 08 June 2010.



12

COE-DAT hosted the **workshop** on “Countering Hybrid Threats Concept Development” on 07-11 June 2010 in Ankara/Turkey. This was the third workshop about the development of the concept about countering hybrid threats. Since July 2009, as a follow-up action from the Multiple Futures Project, Allied Command Transformation (ACT), in coordination with Allied Command Operations (ACO), is developing a new capstone concept for the military contribution to countering hybrid threats. There were 40 delegates from 8 NATO nations, 3 non-NATO nations, ACO and Joint Warfare Center (JWC).

## FUTURE ACTIVITIES



**1** COE-DAT is organizing an **Advanced Training Course** on “Defence Against Terrorism” on 21 September-01 October 2010 in Astana/Kazakhstan. The course intends to analyse the current and future terrorist threat with different dimensions and examine counter-terrorism strategies in detail.

**2** COE-DAT is going to conduct an **Advanced Research Workshop** on “Future Trends in Terrorism” on 11-12 October 2010 in Ankara/Turkey. The workshop intends to elaborate the possible future trends in terrorism in terms of means, methods, ideology and organization with reference to the past and present state of terrorism.

**3** COE-DAT is going to carry out a **course** on “Terrorism and Media” on 01-05 November 2010 in Ankara/Turkey. The course aims to examine media coverage of terrorism, the requirements of media as well as how to deal with media and the best practices in managing information in defence against terrorism.



**4** COE-DAT is going to conduct an **Advanced Research Workshop** on “Maritime Security and Defence Against Terrorism” on 08-09 November 2010 in Ankara/Turkey. The workshop intends to discuss the security challenges in the maritime environment and their likely implications on terrorism by bringing together the subject matter experts, academics as well as the practitioners.





# 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:** info@coedat.nato.int

[www.coedat.nato.int](http://www.coedat.nato.int)