CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM

COE-DAT
Newsletter

Volume 2 / Issue 12 / July-September 2009

Contents

3 General Overview of the Terrorist Activities (July – September 2009)
Ergun ERÜN
LTC (TUR AF)
Gökçen AKYÜZ
Inspector (TUR POLICE)

14 Concept and Governance of Cybercrimes
Hüseyin ÇEKEN
Major (TUR A)

27 The United Kingdom's Counter Terrorism Strategy
Julian CHARVAT
Major (UK A)

37 Strategic Communication For Combating Terrorism Workshop
Aykut ÖNCÜ
Major (TUR AF)
Troy BUCHER
Major (USA A)

47 COE-DAT Activities

50 COE-DAT Publications

COE-DAT:

Your gate to get information.

Editorial

Newsletter's twelveth issue has four main sections. First of all, we share the information and the analysis of the data related to terrorist incidents took place all over the world in the previous three months. Second, we have articles on terrorism related issues. Third, we share the findings of the "Strategic Communication for Combating Terrorism Workshop" which took place on 12-13 May 2009 in Ankara/Turkey. Lastly, brief information about the activities of our centre and its publications are provided in the bulletin.

Maj. Hüseyin ÇEKEN, in his article on Concept and Governance of Cybercrimes provides the reader with an overview of the cyber crimes and possible methods and legislative tools to struggle against them.

Maj. Julian CHARVAT, in his article on The United Kingdom's Counter Terrorism Strategy provides a summary of an updated strategy of The UK for countering international terrorism.

Maj. Aykut ÖNCÜ and Maj. Troy BUCHER, in their report on Strategic Communication for Combating Terrorism Workshop, summarizes the papers presented during the workshop, which brought together academics, experts, and military professionals to improve concepts for using strategic communications in combating terrorism within NATO.

General Overview of the Terrorist Activities (July-September 2009)

Ltc. Ergün ERÜN*

Insp. Gökçen AKYÜZ**

In the third quarter of 2009 terrorist incidents remained at about the same level, totaling 2,808[1] 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.

versus 2,896 during the second quarter of 2009. In this quarter of 2009, 53 countries were afflicted with terrorist attacks, versus 64 in the second quarter of 2009, and the attacks resulted in 5,178 lives lost and 9,301 injured. Also, 434 people were abducted by unknown assailants during this period. The deadliest attack for the quarter was a multiple attack in Baghdad on August 19th in this quarter. A series of blasts in Baghdad killed 95 people and wounded more than 1000 others in Iraq's bloodiest day in 2009. At least six blasts struck near government ministries and other targets at the heart of Iraq's Shi'ite-led administration a month after U.S. combat troops withdrew from urban centers in June, thrusting Iraq's security forces into the lead role. The targets in the attacks were the Rasheed Hotel; the Finance Ministry; the Foreign Affairs, Health and Housing Ministries; the Parliament Building and the Cabinet Building.[2]

Another deadly attack occurred in Mosul on August 7th when a suicide car bomber killed 50 people as they left a Shi'ite Muslim mosque just outside the volatile northern Iraqi city of Mosul. 140 people were wounded in the suicide bombing.

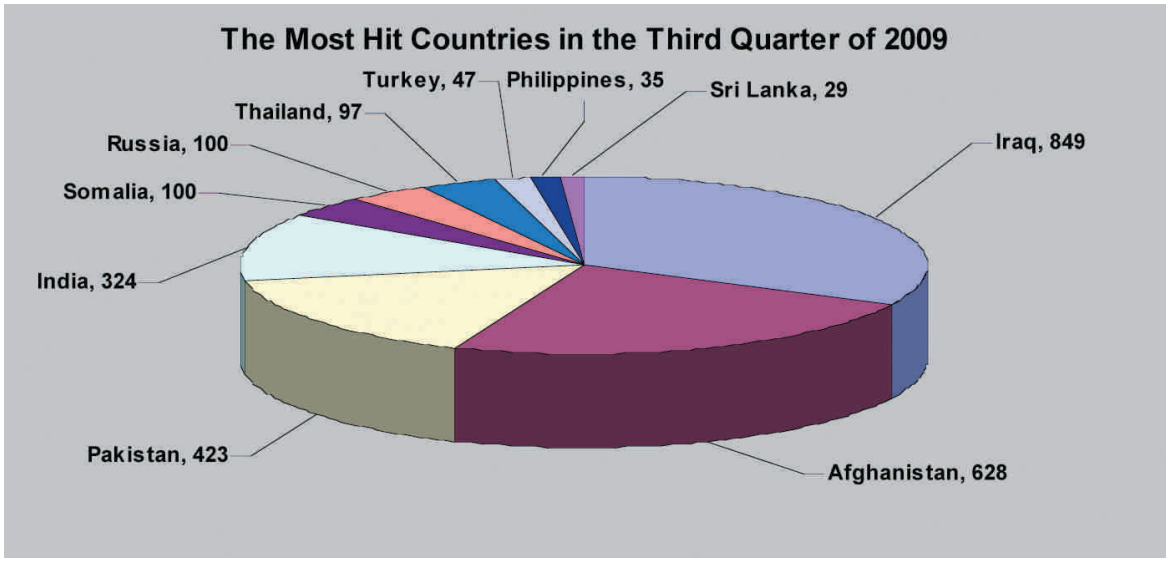
Iraq suffered by far more terrorist attacks than any other country with 849 separate attacks claiming 1,152 lives, injuring 4,423 people, and seeing another 28 persons abducted. The level of violence in Iraq increased roughly 30% from the previous quarter and this quarter accounted for 30% of the total terrorist attacks, 22% of the total fatalities, and 47% of the total casualties for worldwide terrorist incidents. The Iraqi city of Mosul saw the most attacks with 263 separate terrorist incidents claiming 336 lives and wounding 718 people. The second most hit city in Iraq for the period was the capital city of Baghdad with 258 separate terrorist

Simultaneous IED attacks in Baghdad on August 19th claims 95 lives and iniures more than 1000.

*TUR AF, Chief ICMC, COE-DAT
**TUR Police, Analist, ICMC, COE-DAT

[1] 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.

[2] Iraq Map, (accessed October 12, 2005); available from newsimg.bbc.co.uk



Graphic 1 - Worldwide Most Hit Countries in the Third Quarter of 2009

	Country	Event Count	KIA	WIA	AIA
1	Iraq	849	1.152	4.423	28
2	Afghanistan	628	1.325	1.397	106
3	Pakistan	423	905	1.048	44
4	India	324	339	214	61
5	Somalia	100	590	1.011	42
6	Russia	100	199	326	0
7	Thailand	97	91	222	0
8	Turkey	47	30	50	8
9	Philippines	35	97	230	1
10	Sri Lanka	29	5	22	0

Table 1 - The Most Hit Countries Worldwide during third quarter of 2009.

attacks. In Baghdad, the attacks resulted in 472 deaths and 2,573 wounded. The deadliest attack for the quarter occurred in the capital city of Baghdad on August 19th when simultaneous bombs attacks claimed 97 lives and injured more than 100 others.

Violence continued in Afghanistan in the third quarter of 2009 with 628 separate attacks versus 455 in the second quarter, a rough increase of 40%. These 628 attacks claimed 1,325 lives, injured 1,397 and saw 106 people abducted during the period.

The deadliest attack in Afghanistan for the third quarter of 2009 was a Vehicle Borne Improvised Explosive Devices (VBIED) Attack on August 25th. In the attack, some 43 Afghan civilians were killed and 65 others were wounded when a truck bomb was remotely detonated in Kandahar City at dusk. The attack was the worst in Afghanistan in more than a year. The blast flattened several houses and shops in the area and set a restaurant ablaze. The Kandahar bomb also ended a relative lull in violence between the elections and the start of the Muslim fasting month of Ramadan.[3]

[3] Kandahar map (accessed 07 September 2008) available from news.bbc.co.uk/2/hi/south_asia/7602655.stm

VBIED attack in Kandahar province claimed 43 lives and 65 injuries on August 25th

Another deadly attack happened in Kandahar province on September 29th when a roadside bomb struck a civilian bus in the Taliban stronghold Kandahar. In the tragic incident, occurring in the Maiwand district, 30 innocent civilians, including 10 children, seven women and 13 men were killed and 39 others sustained injuries in the incident. The bus was heading from Herat to the capital city Kabul when the tragic incident occurred.

Helmand was the most volatile province in Afghanistan with 65 separate attacks in which 157 people lost their lives, 56 more were injured, and 13 people were abducted. In Kunduz province, there were 47 attacks claiming 104 lives and injuring 49 others, while in Kandahar province 45 terrorist attacks resulted in 189 deaths and 195 wounded. In addition, 33 attacks in Ghazni province resulted in 45 deaths and 110 wounded, while 33 attacks in Herat province killed 63 people and left 125 others wounded. Also, 29 separate attacks in the capital city of Kabul resulted in 67 deaths and 227 wounded. Other provinces inflicted with multiple attacks were Farah province with 25 attacks, Khost province with 25 attacks, Paktika province with 22 attacks, Uruzgan province with 20 attacks, Zabul province with 20 attacks and Logar province with 18 attacks.

In Pakistan violence decreased 10% from the previous quarter. There were 423 terrorist incidents recorded during the third quarter of 2009 versus 473 in the second quarter. These attacks claimed 905 lives, caused 1,048 casualties, and included 44 abductions.

Suicide attacks were at almost the same level in Pakistan during the third period of 2009, but the casualty level decreased roughly 40% in the attacks. For the quarter, 148 people were killed and 496 were wounded in 25 suicide attacks. In the deadliest attack, two suicide attackers separately rammed their explosives-laden vehicles into a Police station in Bannu and a military-owned commercial bank in Peshawar cantonment area of the NWFP on September 26th, killing at least 23 people and injuring around another 200. At least 10 people were killed in the attack in Peshawar, while 13 people, including two Policemen, were

Two suicide attacks caused 23 people dead and 200 wounded in Bannu and Peshawer on September 26th.

killed in the assault on the Bannu Police station. Around 94 people were injured in Peshawar and 64, including 31 Policemen, in Bannu. A car, laden with 100 kilograms of explosives, was used at the site of the Peshawar attack. The suicide bomber sitting inside the car hurled a grenade and then detonated himself and the car. The target was a branch of a bank run by an Army welfare trust. Meanwhile, the Tehreek-e-Taliban Pakistan (TTP) claimed responsibility for the Bannu attack and threatened to unleash bigger attacks on the Government to avenge the killing of their leader Baitullah Mehsud in a US drone attack in August.[4]

Also, another deadly attack was reported in the FATA on August 27th when a suicide bomber struck as Security Force personnel gathered at sunset to break their daily fast. At least 22 soldiers were killed and 10 others injured at Torkham in the Khyber Agency of FATA near the Pakistan-Afghanistan border when a man entered the compound where the soldiers had gathered and blew his self up when they offered to break their fast with him. The bomber targeted soldiers from the Khyber Zakhakhel tribe.[5]

In another attack, an Improvised Explosive Devices (IED) attack in the Punjab Province on July 13th in an eastern Pakistani village killed at least 16 people, including seven children, and injured 70 others. About 100 houses were completely destroyed in the explosion near Mian Channu, a city in eastern Pakistan's Punjab province. About half of the village was affected by the blast and many houses were

Suicide attack in FATA, Kyber Agency claimed 22 lives and 10 injuries on August 27th.

4 Bannu map (accessed 05 August 2004) available from news.bbc.co.uk/2/hi/south_asia/3537740.stm,
5 Kyber Agency map (accessed 26 August 2004) available from news.bbc.co.uk/2/hi/south_asia/3597478.stm

IED attack in Punjab province killed 16 people and wounded 70 others on July 13th.

caved-in, trapping more people inside. Mian Channu is not far from the Punjab capital of Lahore, which has been a target of several militant attacks in recent months. The largest attack targeted the visiting Sri Lankan cricket team in March, leaving seven people, including five policemen, dead and six Sri Lankan players injured. This quarter's deadliest attack in Pakistan occurred at the house of a school teacher where 40 to 50 students were studying, leaving most of the children still unaccounted for. There was no sign of a suicide attack, but the blast was tremendous, leaving a 40-foot wide and 8-foot deep crater at the site of the detonation.[6]

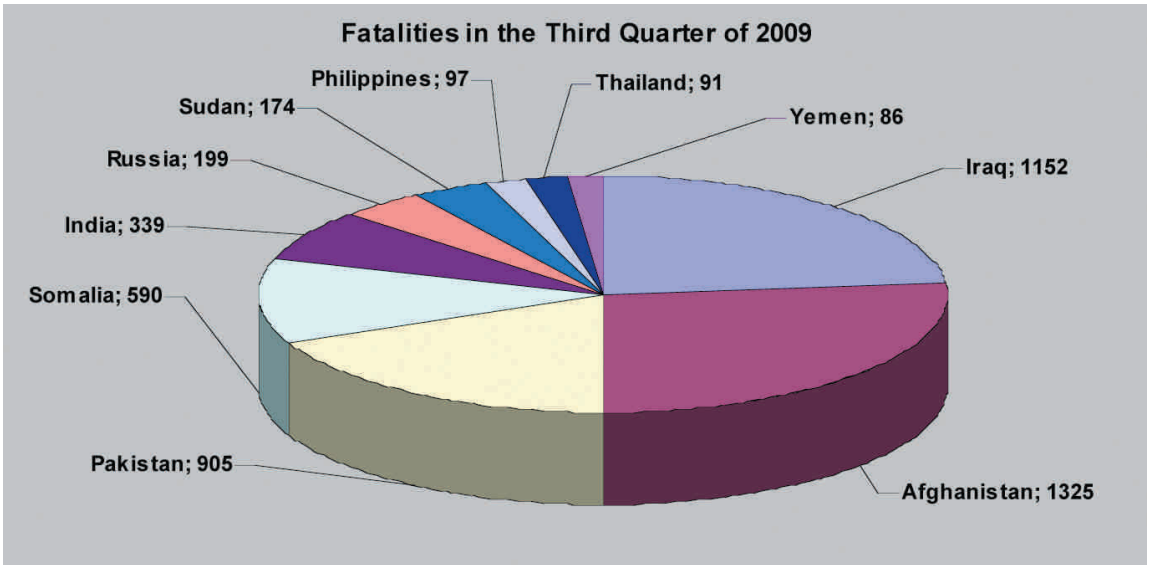
India saw the fourth most terrorist attacks in the world according to number of attacks carried out for the third quarter of 2009 with 324 attacks. These attacks claimed 339 lives and caused 214 injuries in sum, and there were 61 abductions by unknown assailants.

The deadliest attack was a clash in Chhattisgarh province on July 12th. In two incidents in the Rajnandgaon District the Cadres of the banned Communist Party of India-Maoist (CPI-Maoist) killed 36 Police personnel, including a Police Superintendent.

Also, another major attack in August 2009 was an armed attack in the Chhattisgarh province. Eight members of a family, including a two-year-old girl, in the remote Koilibeda area of Kanker District were killed by the Communist Party of India-Maoist (CPI-Maoist) on August 12th.[7]

At least 36 policemen killed in a clash in two separate incidents in Chattisgarh on July 12th.

[6] Punjab map (accessed 02 April 2009) available from ws.bbc.co.uk/2/hi/south_asia/7979022.stm
[7] Chattisgarh map (accessed 30 April 2006) available from www.dhivehiobserver.com/archives/index16-30Ap...



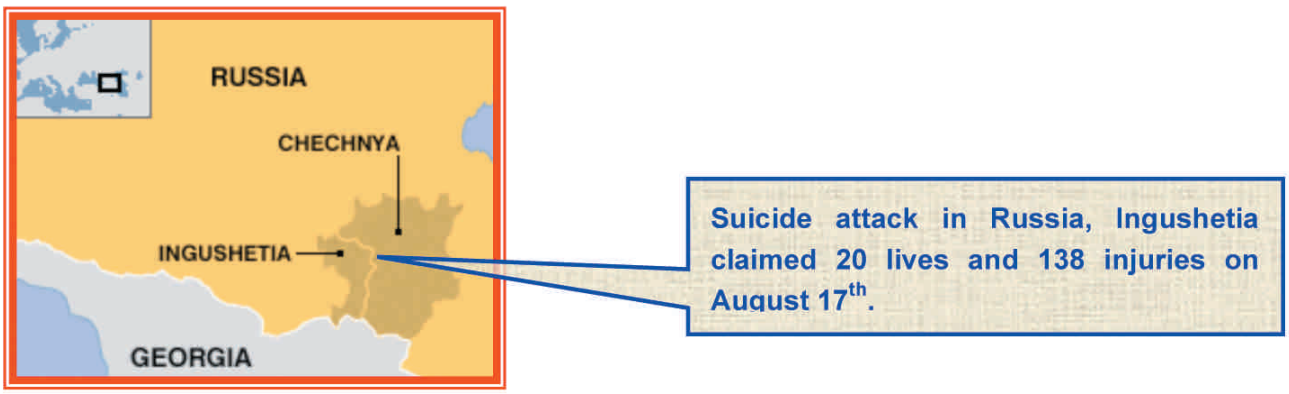
Graphic 2 - Ten Countries Those Gave the Highest Fatalities in the Third Quarter of 2009

Terrorism related violence in Somalia claimed 590 lives and injured 1,011 others in 100 separate attacks, making Somalia the most targeted country in Africa. According to the data available, terrorism related incidents decreased roughly 25% in the third quarter of 2009 in comparison with the previous quarter. The most deadly incident was an IDF Attack on July 23rd when heavy shelling targeted parts of Mogadishu, the Somali capital, claiming 25 lives. Several shells landed in the neighborhoods of Wardigley, Bondere and Karan districts in the north of the capital. Another deadly attack was an IDF Attack on August 21st when heavy shelling targeted parts of Mogadishu, the Somali capital, claiming 40 lives and wounding more than 100 others.

There were twelve different tactics used by terrorist in Somalia during the period, with clashes being the most frequent with 40 separate incidents killing 372 people and wounding 574 others. Armed attack was the second most used tactic with 13 separate incidents claiming 22 lives and injuring 34 others. Other tactics used in Somalia during the quarter were abduction, arson, execution, Indirect Fire (IDF) attack, Improvised Explosive Devices (IED) attack, piracy, raid, suicide attack, and the Vehicle Borne Improvised Explosive Devices (VBIED) Attack.

Violence in Russia increased not only compared to the previous quarter, but also to the same period in 2008. There were 100 separate terrorist incidents during the third quarter of 2009, resulting in 199 deaths and 326 wounded. The most significant attack in Russia occurred in Ingushetia on August 17th. A total of 20 bodies were found at the site of a powerful bombing that rocked the city's Interior Department in central Nazran, the regional capital of Russia's turbulent North Caucasus Republic of Ingushetia. Six of the 20 bodies have been identified, and 138 people were hospitalized. In the incident, a suicide bomber, driving a Gazelle, rammed the gate of the City Interior Department, drove into the courtyard and activated the bomb in his vehicle. The powerful bomb was estimated to be equivalent to one ton of TNT,

leaving a crater 4 meters wide and 1.5 to 2 meters deep, and creating a huge fire with heavy smoke.[8] Ingushetia map (accessed 31 October 2008) available from news.bbc.co.uk/2/low/europe/7701752.stm Armed Attack was the most used tactic during the quarter with 31 occurrences while 25 IED Attacks, including two VBIED Attacks, was the second most used tactic. The most remarkable development in Russia was an increase in suicide attacks. Eight suicide attacks, versus two during the previous quarter, claimed 35 lives and injured 154. Other methodologies used in Russia during the quarter were clash, execution, Indirect Fire (IDF) attack, raid and Vehicle Borne Improvised Explosive Devices (VBIED).



Violence in Thailand increased approximately 20% during the third quarter of 2009, with 97 separate attacks compared to 80 during the previous quarter. The attacks for this quarter resulted in 91 deaths and 222 wounded. The three troubled southern provinces, Pattani, Narathiwat and Yala, were the most volatile cities in terms of the number of attacks carried out during the period. Pattani suffered 34 attacks that resulted in 30 people killed and 86 others injured while in Yala 36 people were killed and 40 were wounded in 31 separate attacks. The province of Narathiwat also suffered a significant number of attacks, 25, which claimed 21 lives and wounded 73 others. In the largest attack, five military rangers were killed in Thailand on September 13th when an armed group attacked their base in Yala, a province in the far south that has seen an upsurge in separatist violence. The attack on the base in Muang district came in the early evening and lasted about 10 minutes. The base is located in a remote area away from the civilian population. In terms of the incident

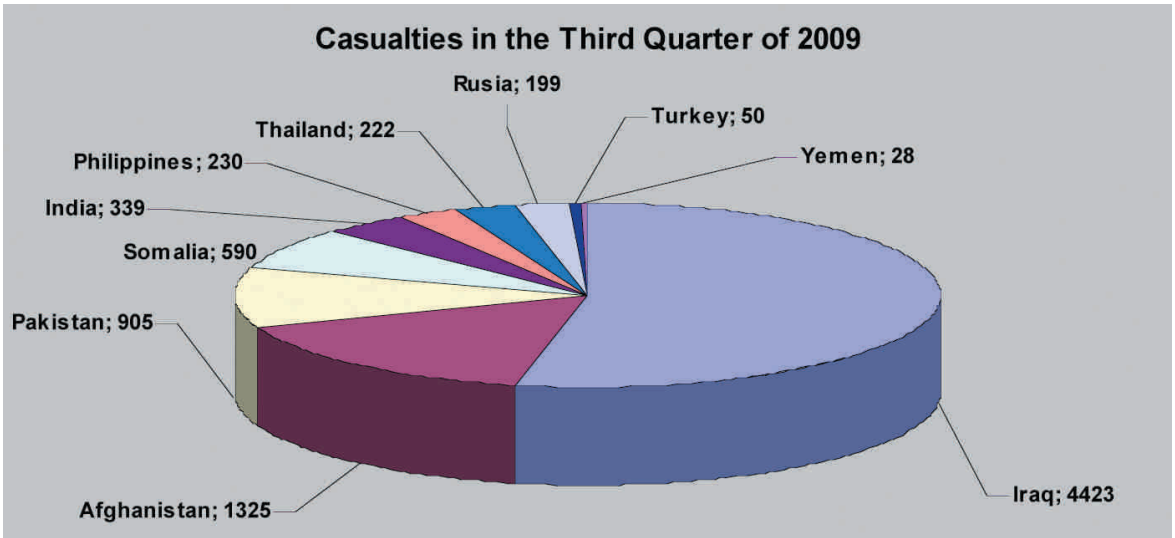
[8] Ingushetia map (accessed 31 October 2008) available from news.bbc.co.uk/2/low/europe/7701752.stm

type, the traditional armed attack was the most used tactic in Thailand, with 55 separate attacks claiming 69 lives and injuring 45, while the second most used tactic, with 27 repetitions, was IED attacks, causing the death of nine people and wounding 89 others during the quarter.

Turkey was the eighth most hit country in the world during the third quarter of 2009 with 47 separate terrorist attacks conducted by PKK/KONGRA-GEL terrorists. These attacks claimed 30 lives, caused 50 injuries, and included eight abductions. The most deadly attack happened in Siirt on September 8th. Five soldiers were killed during a clash between security forces and PKK/KONGRA-GEL terrorists and three others were wounded in the clash. Seven different methodologies were used in Turkey by terrorists in the third quarter of 2009. The most used one being the IED attack with 20 repetitions that included two Victim Operated Improvised Explosive Devices (VOIED) attacks. The IED attacks resulted in 17 deaths and 31 wounded, while 15 clashes killed 12 security personnel and wounded 16 others. Also, four abductions, six arson attacks and one IDF attack occurred during the period. In terms of the provinces, Hakkari was the most hit with 17 attacks claiming seven lives, causing16 injuries, and having two abductions. Also of note, 11 terrorist attacks in Sirnak killed nine people and left 20 others wounded. Other provinces hit during the quarter were Adiyaman, Batman, Bingol, Diyarbakir, Hatay, Istanbul, Mardin, Siirt, Tunceli and Van.

Violence decreased roughly 60% in the Philippines for the quarter, with only 35 attacks. However casualty rates were still high with the attacks claiming 97 lives and wounding 230 people. Also, there was one person abducted during the third quarter of 2009. The deadliest attack was a clash on August 12th. Twenty-three government troops lost their lives in a day of intensive skirmishes in the southern Philippine jungles. Hundreds of troops stormed two camps of the Al Qaida-linked Abu Sayyaf group in the southern Basilan province. Sporadic firefighting broke out in the pre-dawn hours and continued until late into the night. Another deadly attack was an IED attack on July 7th when two separate blasts rocked the normally restive southern Philippines, killing six civilians. In the first blast, an improvised bomb attached to a motorcycle went off in front of a store in Jolo, in the Sulu province, killing two civilians and wounding approximately 40 others, including three policemen. After the blast, two more unexploded improvised explosive devices were recovered by bomb experts. Only three hours later, another bomb in a 1987 model Mitsubishi Lancer car, exploded in the southern Iligan City, injuring 13 people, including three government soldiers. In terms of methodology, armed attacks were conducted 12 times, claiming 26 lives and wounding 19, while clashes occurred 10 times resulting in 43 deaths and 29 wounded. In addition, nine IED attacks claimed 24 lives and injured 156 while three IDF attack resulted in four deaths and 26 wounded. Lastly, a civilian was abducted in Basilan province on July 28th.

There were 29 separate attacks in Sri Lanka that claimed five lives and injuried 22 during the third quarter of 2009. In general, clash, close quarter armed attacks, Improvised Explosive Devices (IED) attacks and indirect fire were the predominating tactics used by the terrorists in Sri Lanka. The most used tactic was the IED attack with 21 repetitions including four Victim Operated Improvised Explosive Devices (VOIED) attacks that killed one person and wounded 14 others, while the IDF attack was the second most used tactic with two occurrences. Of note, two armed attacks killed two people in Sri Lanka. Other methodologies used in the country were arson attack, clash and suicide attack.



Graphic 3 - Ten Countries Those Gave the Highest Casualties in the Third Quarter of 2009

In Europe eight countries, including Russia, were attacked by terrorists during the quarter. The most attacked country was Russia with 100 separate attacks while Turkey was the second one with 47 separate attacks during the quarter. Also, in Georgia, three separate attacks occurred during the quarter killing three and injuring ten, while Spain was attacked three times, killing two civilians and wounding 46 others. Other countries that had terrorist attacks during the quarter in Europe during the quarter were Greece, Kosovo, Serbia, Spain and United Kingdom (UK).

Throughout the world, terrorists used 14 different tactics in the third quarter of 2009. IED attacks were the most used tactic during the quarter with some 952 attacks claiming 1,226 lives and wounding 2,912 others. Traditional armed attacks were the second most used tactic during the quarter with some 725 occurrences resulting in 1,189 deaths, 580 wounded and 28 people abducted. Iraq saw the most IED activity, suffering 409 separate attacks. Afghanistan saw the second most IED attacks with 246 incidents, while Pakistan was the third with 100 IED attacks. Also, 52 IED attacks were reported from India and 27 IED attacks were reported in

Thailand. The deadliest IED attack occurred in Kandahar province when at least 30 people were killed in a bomb blast on September 29th. A roadside bomb struck a civilian bus in Taliban stronghold Kandahar province killing 30 innocent civilians while 39 others sustained injuries in the incident.

Extrajudicial killings posed an important security challenge for Afghanistan, Bangladesh, India, Jamaica, Pakistan, Russia, Somalia, Thailand and especially for Iraq where 164 people lost their lives in captivity in 73 separate incidents.

	Event Type	Event Count	KIA	WIA	AIA
1	IED	952	1.226	2.912	1
2	Armed Attack	725	1.189	580	28
3	Clash	450	1.285	1.351	33
4	IDF	210	346	848	0
5	VBIED	132	498	2.394	0
6	Suicide Attack	97	474	1.159	0
7	Abduction	72	1	1	311
8	Arson	71	12	18	11
9	Execution	44	90	5	3
10	Raid	29	49	21	9
11	VOIED	9	7	8	0
12	Piracy	6	1	4	38
13	Hoax	6	0	0	0
14	Cyber Attack	2	0	0	0

Table 2 - The Most Used Tactics in the World during the Third Quarter of 2009.

In addition, the clashes between security forces and terrorists caused considerable damage with 1,285 people losing their lives, over 1,351 sustaining injuries, and with 33 abducted in 450 separate incidents.

The wide use of Indirect Fire (IDF) attacks was also noted during the quarter, killing 346 and wounding 848 in 210 attacks.

The Vehicle Born Improved Explosive Devices (VBIED) was the fifth most used tactic. There were 132 separate attacks claiming 498 lives and injuring 2,394 during the quarter. Iraq was the most afflicted with 112 separate VBIED attacks that killed 399 people and wounded over 2,172. Other countries with attacks using this tactic during the quarter were Afghanistan, Georgia, India, Indonesia, Pakistan, Russia, Somalia, Spain and Thailand.

Suicide Bombing was the deadliest form of IED attack with 97 incidents killing 474 people and wounding 1,159 others during the third quarter of 2009. Afghanistan was the most volatile country according to the data available on suicide attacks with 40 separate attacks. Pakistan suffered the second most suicide attacks with 24 attacks. Iraq was the third hardest hit by this tactic, suffering 19 such attacks. Other countries targeted were Russia with eight, Somalia with two, and Indonesia, Mauritania, Saudi Arabia and Sri Lanka afflicted with at least one each during the quarter.

Abductions were another tactic used during the period. In some 72 attacks were the primary purpose was abduction, there was one person killed and another wounded in the course of assailants kidnapping 311 people during the quarter.

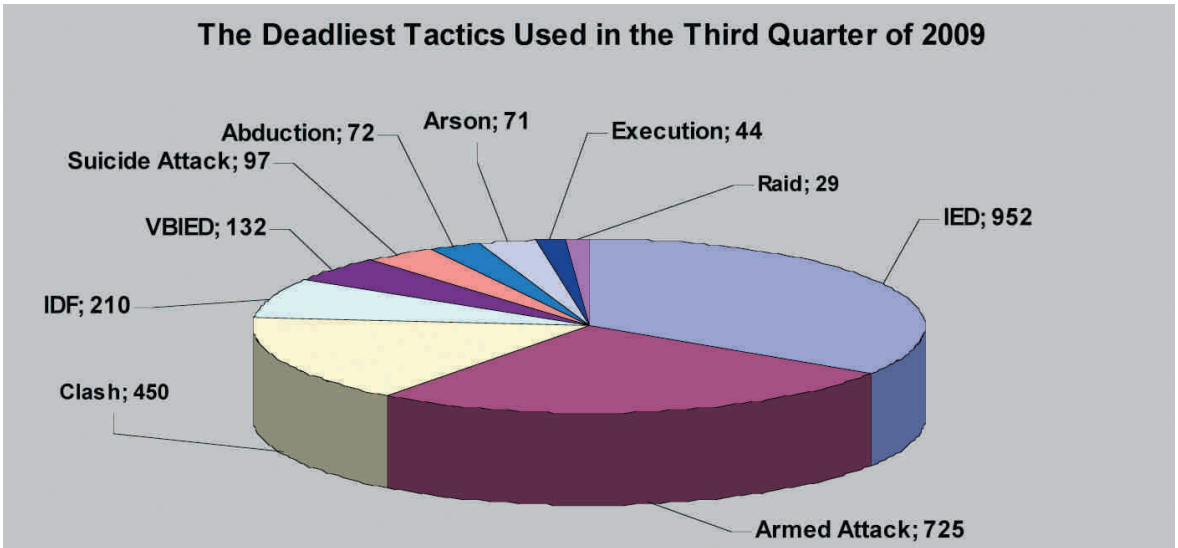
There were 71 arson attacks this quarter that resulted in 12 deaths and 18 wounded, and saw 11 persons abducted during this type of attack. India was the leading country with 24 arson attacks while Pakistan was second with 16 attacks.

Execution was the ninth most used tactic during the quarter with some 44 incidents claiming 90 lives. Pakistan was the most volatile country related to execution with 15 incidents that resulted in 41 deaths. Iraq was second with nine incidents. Also, Afghanistan, Bangladesh, India, Nigeria, Russia, Somalia and Thailand were countries that had at least one execution occur during the period.

Raid was the tenth most used tactic during the second quarter of 2009 with 29 separate attacks claiming 49 lives, wounding 21, and having nine abductions. Afghanistan had the most occurrences with 12 separate raids. Iraq and India both had three of these attacks. In addition, Bangladesh, Democratic Republic of Congo (DRC), Nepal, Nigeria, Pakistan, Peru, Russia, Somalia, Sudan and Tajikistan were the other countries afflicted with raids during the quarter.

The Victim Operated Improvised Explosive Device (VOIED) attack was the eleventh most used tactic for the period with nine attacks claiming seven lives and injuring eight others during the quarter. Sri Lanka suffered the most VOIED attacks with five attacks that caused six injuries. Also, Afghanistan, India and Turkey saw VOIED attacks during the third quarter of 2009.

Last, there were six occurrences of piracy, six hoaxes and two cyber attacks reported during the third quarter of 2009.



Graphic 4 - The Deadliest Tactics Used in the World in the Third Quarter of 2009

Concept and Governance of Cybercrimes

Maj. Hüseyin ÇEKEN*

In today's world, we live in a period where humanity is getting more and more liable to the information technology. Computers and information systems that are consisting of digital technology are unavoidable parts of our lives and humanity is getting more and more dependent on these technological instruments, day by day. From entertainment to banking, to medicine, to health and to many other fields in our lives, they are inevitably challenging. The most important feature of this proliferation is the Internet. Today Internet is taking the form of an information superhighway no matter useful or not, almost every kind of information can be utilized in private homes by just pressing fingers on some keystrokes.[1]

"The development of the Internet has created new techniques and capacities for individuals to use as they join in the complex interactions of their daily lives, it can be whether entering into consumer and commercial transactions, gathering information, participating in political debate and action, doing work, or communicating as part of their personal and intimate relations. At the same time, the Internet is one manifestation of the groundswell of digital technologies which pose major challenges for our conceptions of how people should govern themselves. Debates are overwhelming about the role of territorial based governments, the efficiency of traditional legal techniques, the desirability for new forms of self-regulation, and the need for international cooperation. Today, cyberspace strikes many hard questions on how best to facilitate relationships and transactions, to protect people from harm, to encourage democratic practices, and to ensure fundamental rights and freedoms. Cyberspace also raises fears among some about the ungovernability of harmful conduct including such activities as illegal interception of telecommunications, electronic vandalism and terrorism, stealing telecommunications services, pornography and other offensive content, telemarketing fraud, money-laundering, and telecommunications in furtherance of criminal conspiracies."[2]

Despite very precious benefits it makes available, the cyberspace which hosts Internet, can also be a real disaster. Especially this is the case when cyber potential is used as means of perpetrating crimes. Modern information and communication systems make it possible to commit illegal activities at any time, from one place to another in the world.

Extraterritorial nature of those illegal acts, makes it quite hard to pursue, arrest and penalize the perpetrators of crimes. In other words, dependency on Internet and other information technologies bears a great risk for information society. This risk should be handled and removed with the utmost care so that both availability of cyberspace

*TUR A, LEGAD, COE-DAT

[1] Ulrich Sieber, "Legal aspects of computer-related crime in the information society -comcrime study", p. 59. http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html (17.11.2002).

[2] Michael Mc Neill, "Governance of cyberspace : canadian reflection: prepared for law, regulation and governance" http://www.carleton.ca/~mmacneil/118/1999/draft-macneil-cyber.htm_(24.11.2002).

and the integrity of society should be balanced simultaneously.[3]

Regarding the Internet as not a "lawless" place, Criminal Law can be one of the pillars in reaching this goal. But as an instrument, traditional Criminal Law approaches may not yield us to the objective. In other words, Criminal Law should be equipped with some extra procedural tools on which fighters should compromise.[4]

II. CONCEPT AND GOVERNANCE OF CYBERCRIMES

A. DEFINITION

Users in the Internet found a spiritual way to express their communications across the Internet. They named this phenomenon as “cyberspace”. The coining of the word “cyberspace” has been first done by science-fiction writer William Gibson. He wrote a book named "Neuromancer", in 1984. The book was telling a future in which the information infrastructure prevailed and information was more valuable than money. It involved huge companies instead of governments and computer users who challenged war against secure data and information. The thing making this a spiritual and somewhat prophetic work was the settings which had no physical existence. He named this phenomenon as "cyberspace".[5] "Cybercrimes are the offences which are perpetrated across cyberspace including computers and/or information technologies in any step of criminal activity. The terms 'computer crime', 'computer-related crime', 'high-tech crime', 'internet crime' and 'cybercrime' are often used one for another. Generally the word 'computer-crime' has two elements that are 'computer' and 'crime'. Therefore it can be defined in its simplest form as 'a crime in relationship with computers'. The relationship between 'computer' and 'crime' either be direct or indirect form. For example, if a perpetrator uses or manipulates a third user to reach at his criminalistic goals, the relationship between two is indirect, because, in this case, perpetrator does not solely use his computer, but he also deceives someone else and uses someone else's computer."[6]

Nevertheless, a difference could be driven between computer specific crimes and traditional crimes that are performed with the help of computer technology. The most usual instance of this can be seen in the Customs Law, in which the Internet proves to be a good means for committing crimes against Customs Law, such as smuggling, counterfeit, etc. On the contrary, the computer-specific crimes demand up to date versions of the definitions of crimes in national penal codes, the traditional crimes performed with the help of computers demand improved

[3] Sieber, ibid, p.193.
[4] David Wall & Clive Walker & Yaman Akdeniz, The Internet, Law and Society, Pearson Education Limited, p. 16, UK, 2000.
[5] Brett Burney, "The concept of cybercrimes- is it right to anologise physical crime to a cybercrime?", http://cybercrimes.net/Virtual/Burney/.html (17.11.2002).
[6] Allen Hammond, "The 2001 Council of Europe Convention on Cybercrime: an efficient tool to fight crime in cyberspace?", http://www.magnin.org/Publications (17.11.2002).

collaboration and procedural measures.[7]

"The history of 'computer crime' goes back as far as to the 1960s when first writings related to the cases of 'computer crime' or 'computer-related crime' were issued in the journals. These cases basically, involved computer misuse, computer sabotage, computer espionage and the outlaw usage of computer systems. The first scientific crime studies began approximately in 1970s. These works enlightened a limited portion of computer crime cases. The usual and scientific aspects of computer crime abruptly changed in 1980s. This especially when the journals made heard interesting cases about hacking, viruses and worms. Meanwhile, a broad violation of piracy in computer programs, misuse of cash dispenser and telecommunication abuses showed to public the weakness of the information society. It was soon later than those developments that the new challenge was threatening all kinds of legal interests, such as the manipulation of a hospital computer or computer-related violations of privacy. Hence, it became clear that the problem had to be handled more seriously. Later in the 1990s, Internet became a means of distributing illegal contents and began to be utilized as tools for conducting organized crime. In 1983, a group of experts of the Organization for Economic and Commercial Development (OECD) made a definition towards the term 'computer crime' (or 'computer-related crime') as 'any illegal, unethical, or unauthorized behavior involving automatic data-processing and/or transmission of data'. Later in its 10th Congress in Brussels (2000) United Nations reached another definition describing computer-crimes as "any act aiming to give harm to the security and functions of computers". United Nations also declared another definition at this Congress, for so called cybercrimes or Internet crimes as 'any unlawful act committed against and inside any other computer or network systems' ".[8]

As we understand from United Nation's definitions, United Nations treats cybercrimes in two different groups: in the first group, there are narrow scope cybercrimes which are mainly computer-crimes, and in the second category, wide scope cybercrimes which are committed via computer or network systems. In our thesis, we will deviate from this dual approach of United Nations and accept that the term "cybercrimes" covers and involves the term "computer-crimes".

Nowadays, the availability presented by Internet, constitutes the core of any cybercrime issue, and the Internet itself can be defined as the network which is comprised of networks. Basically, it is an still-growing network of connected computers that are connected to other systems. However, Internet is something more than that. The characteristic of it is illustrated as “cyberspace”

[7] Communication from Commission of European Communities to European Union Dated 26.01.2001, http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html (17.11.2002).

[8] Sieber, ibid, p. 19-20.

which has constituted a real medium that involves not only the Internet, but other types of networks including phone and satellite networks. The Internet is just only a small portion of cyberspace, but there is a strong tendency to accept both as the same.[9] In other words the term "cyberspace" has wider meaning than the word "Internet". For this reason, the term "internet crime" can not specify the problem in the best way, due to its respectively narrow meaning. Internet is just a part or one of the parts of the cyberspace. However, we should accept that it is at the same time, the most preferred form of communication taking place in cyberspace.

Besides Internet, there are LANs (Local Area Networks) or WANs (Wide Area Networks). These are called as "Intranet" because of their closed end constructions. For example a closed network system founded for military or finance objectives, in order to lower cyberthreat can be defined as "intranet". The communication going on this kind of intranet bodies is also a part of cyberspace and any unlawful behavior taking place through them is specified as cybercrime. For this reason, we believe the term "cybercrime" has the widest meaning and fits the problem in the best way. If we want to formulate it, we can deduce that "not every cybercrime is an internet crime but every internet crime is a cybercrime". [10]

Within this concept, Cybercrime Convention that we will focus on in forthcoming chapters also accepts the term "cybercrime" just as the way we do.

B. A COMPARISON BETWEEN CYBERCRIMES AND CLASSICAL CRIMES

Penal Law deals with preservation and protection of valuable legal interests. Emergence of new types of legal interests always brings protection provided by Penal Law. In recent years developments in the information technology have brought about new legal interests.[11] Computers and information technologies are one of those interests. Developments in information technology have let great economic and social changes, but they also have a side affect: the emergence of new types of crime as well as the commission of traditional ones, by means of new technologies. Moreover, the results of criminal behavior can be more disastrous than before, because they are not confined to national boundaries any more.[12] For this reason, new counter-measures should be put into practice for the sake of mankind.

Those crimes usually emerge as unauthorised access and abuse of bank and hospital records, military espionage, hate speech, defamation, child pornography, terrorist propagation, gambling, burglary, embezzlement, fraud, vandalism and violation of privacy. As we see,

[9] Burney, ibid.
[10] Hasan Sınar, Internet ve Ceza Hukuku, Beta Publishing, p. 69, ‹stanbul, 2001.
[11] Yener Ünver, "TCK ve TCK tasarısının Internet aç›sından de¤erlendirilmesi", ‹ÜHFM, Vol. LIX, No: 1-2, p.51-52.
[12] Explanatory Report of CoE's Convention 2001 on Cybercrimes, p.2, http://www.c4group.net/ivhp/bilgibelge/docs/Explanatory%20Report.doc (17.11.2002).

all these actions are violating classical interests. Nevertheless, beside these classical actions there are also some new varieties of crime models such as, computer and data interception, data interference, infringements of intellectual property rights, vandalism towards important materials for public, forgery in identification cards, spamming, cyberstalking, money laundering, and fraud by credit cards.[13] For this reason, it is quite disputable whether cybercrimes are a new and different category of crimes or they are just a simple variation of traditional crimes. The answer of this question will lead us in deciding whether the cybercrime regulations should be held within the penal codes or within some other statutes.

A crime is said to be complete when someone involves in activity (or a non-activity) which is “socially intolerable”. Criminal law is a tool to prevent the “bad consequences” or “injurious effects” or simply the “harm” that is caused by socially intolerable activities. An activity can not be accepted as a “crime” unless there is a preceding law or statute that precisely illustrates the criminal conduct and sets forth a punishment. But things are a little bit different in cyberspace. For example, the physical crime "burglary" demands a person physically breaking and entering into ones house.[14]

If we draw main elements of physical "burglary" to cyberspace, for instance, if a computer user in Istanbul, remotely accesses a computer in Ankara, the only thing that enters” into the computer in Ankara are digital bits which are one's and zero's. In this situation, perpetrator solely sends digital bits into space. If we claim that burglary in cyberspace is not a crime, then some would argue that a person shooting a gun is not guilty either. Because, someone might claim that "the man was killed by the simple bullet, not by the man who pulled the trigger". Indeed, it is the bullet that travels through the space and causes a penetration in a physical person's body.[15]

In case of applying physical crimes such as "burglary" to cyberspace, then we have to point out a perfect similarity between the physical goods and cyberspace goods. Here it seems that we have two alternatives: either, implement present criminal law to cyberspace, or establish some other grounds. If burglary can be committed in physical space by the act of walking and the movement necessary to “break” into property, then the digital bits are equivalent to walking and physical movement. However, things in cyberspace is not that easy.[16]

We share the view that it is appropriate to analogize crimes in physical space and cyberspace. As we mentioned above, most of the cybercrime models are either the same or very similar to that of classical crimes executed in the physical world. For this reason, cybercrime regulations should be handled in articles related to classical crimes as the aggravation

[14] Burney, ibid.
[15] ibid.
[16] S›nar, ibid, p. 71-72.

conditions of those crimes.[17] For example a forgery act by using computers should be an aggravation condition of classical forgery offence due to the difficulty in conceiving the forgery committed, but on the contrary, due to the easiness in perpetrating the act of forgery.[18]

The most famous example shown by those who believe that there is a peculiar category of cybercrimes happening and resulting completely in cyberspace and for that reason, these crimes should be categorized as "real virtual crimes", is the so-called virtual rape event that happened in a computer game called "Lambda MOO".[19]

In fact, this game was just a fake and could never be accepted as a real rape event. In the game, perpetrator, Mr. Bungle who was one of the participants had written some special computer code (voodoo doll) and had caused other players conceive that mistreated lady players was in conformity with the cyber-rape that they were exposed to.[20]

In this example, the criminal conduct was not the same as that of a physical rape, on the other hand, this unlawful action could be handled as defamation or mentally tort of the physical world.[21]

Consequently, we treat cybercrimes as a different aspect of classical crimes but not a special and brand new category of crimes, because in most forms of cybercrimes, the legal interest remains the same when compared to that of classical crimes. However, due to easiness in perpetrating crimes and complexity in detecting perpetrators, those crimes should be handled with heavier sanctions which were expressed as conditions of aggravations in usual penal codes.

C. ALTERNATIVES FOR TREATING AND GOVERNING CYBERCRIMES

1. Governance In General

Internet was first developed and designed for military purposes, then it was began to be utilized by the American academic institutions and later on, usage of that was transferred to academic communities in other developed countries. Today it has people using it all over the world, from almost every age group. Furthermore, today it can be reached by even a young boy from her bedroom at any time he wants. Nevertheless, this infant is exposed to all kinds of exploitation, while surfs in the net. In such cases, we must have some other instruments, in order to overcome intolerable activities on the Internet and find some ways for letting end-user control of what is accessible on the net.[22]

[17] Ünver, ibid, p. 87-89.
[18] U¤ur Alacakaptan, Announcement he made in Panel, on "Internet and Penal Law Issues", 16 March 2002, Istanbul Bilgi University.
[19] For detailed information about the rules of the game see : Jennifer L. Mnookin,"Virtually law: the emergence of law in lambdamoo, journal of computer-mediated communication", http://www.ascusc.org/jcmc/vol2/issue1/lambda.html (17.11.2002).
[20] Sınar, ibid, p. 74-75.; Susan Brenner, "Is there such a thing as virtual crimes?", http://boalt.org/CCLR/v4/v4brenner.htm (14.11.2002).
[21] Ünver, ibid, p. 80 ; Sınar, ibid, p. 77.
[22] Roger Darlington, "Should the Internet be regulated?" http://www.rogerdarlington.co.uk/regulation.html (17.11.2002).

Nowadays, Internet is the strongest means of broadcasting information and conducting trade but, some people utilize it for a wide range of unsocial and unlawful activity. Most of those disseminations are accepted as illegal in almost every country, all over the world. Such activities usually include, copyright violations, misuse of credit cards, financial scams, hacking, money laundering, military espionage, cyber-terrorism, real-time terrorism, cyber stalking. Society has the right to protect itself by defining those bahaviours crime.[23]

It is strongly claimed that any system for watching the content disseminated across the Internet will consequently cause a violation for the individual's right to freedom of expression which is characterized as obsolute and deprivation of which causes irrepairable damage to notion of civil liberties.[24] It is indisputably true that, the need to provide individual's freedom of expression in a civil society is of highest importance and any efforts made for watching Internet must take these points into consideration.[25] However, almost all groups of fundamental rights have to be qualified, otherwise, they will threaten other rights. If we turn to our issue, an unlimited right to freedom of expression might threaten the right of children to be free from child-pornography and the right of minorities to live their lives without racial discrimination and violence.[26] For this reason, we believe cyberspace is not completely a "lawless" environment and should carefully be regulated so that mankind's benefits are to be maximized.

By the way, there will inevitably arise some disputes between people, as they get in touch and do trade through Internet. Still, many people hope that the new online community can handle things out informally, by using "netiquette" or social pressures, instead of rules to prevent harms and settle disagreements. However, every day many many more new users participate the net and as the monetary structure of the net increase, and it seems possible that some other rules will be necessary, and some enforcement of those rules will be demanded. The essence of the problem is that, where those rules will emerge from and who will follow the reinforcement of them.[27]

Some of us might argue that, we should not care for the present territorial governments but should create a self-regulatory regime instead that is specified and supported by system operators and users who are fluent with this new media in the best way. An answer to this question, whether cyberspace should be self-regulating or not, is to discuss in detail, how the law of cyberspace can be emerged and enforced so as to

[23] ibid,
[24] Özgür Uçkan, "Internet ve 'düzenleme' kavramı üst kurullar ve ifade özgürlü¤ü", http://www.c4group.net/ivhp/bilgibelge/docs/internet&hukuk_uckan.doc (10.11.2002).
[25] Yaman Akdeniz, "Who watches the watchmen?", Filters and Freedom: Free Speech Perspectives on Internet Content Controls (Ed. David L. Sobel), p.33-50, USA, 1999.
[26] Darlington, ibid.
[27] David R. Johnson, "Lawmaking and law enforcement in cyberspace", http://www.cli.org/DRJ/make.html (17.11.2002).

reach at both effectiveness and justice.[28]

Basically, there are four competing alternatives for governance of cyberspace, the first three of which are said to be traditional models, though, the fourth model is untraditional, and decentralized. The fourth model calls for regulations be proposed to originate from the ethical beliefs of people who use cyberspace. That' s why, another nomenclature for the fourth model is self-regulatory model. Below we will examine each alternative one by one.

1. Competing Models

a. Nationality Based Governance

This model is the oldest and most classical one which is mainly based on geographical features of the nation-states.

"This is a model where existing territorial sovereigns can simply seek to extend their jurisdiction, and to amend their national laws as they feel necessary, to attempt and govern all actions on the net that have substantial impacts on their own citizens. The non-geographic character of cyberspace makes it very difficult to apply current, territorially-based rules to activities online. Local sovereigns may have a monopoly on the lawful use of physical force, but they cannot control online actions whose physical location is not relevant or can not even be established. This model inheres the risk of overly aggressive regulation that operates to drive disfavored activities 'offshore'. In other words, national legislative bodies might arbitrarily make so aggressive regulations and enforce these regulations that they might penetrate other nations' jurisdiction. These over-regulations might also yield as to disconnect the local territory from the new, valuable environment of global trade. The problem with using existing territorial governments as the source of rules for activities taking place in cyberspace is not only that such rules are unlikely to have universal, long-term impact; but also is that, no existing sovereign possesses the legitimate authority to make such rules. This model of governance represents, in effect, an extra-territorial power grab when transposed to cyberspace, a form of colonialism long rejected in the non- virtual context. Furthermore, the political institutions of established sovereigns are usually not well suited to create wise rules for the net. For instance, rules of any national sovereign for online conduct, even if they are reached at democratically, might not take into consideration the interests of all who are affected by those rules in case of their implementation in the online world. By the way, no country's efforts to 'plant its flag' on the cyberspace and in effect declare sovereignty over cyberspace is more clearly grounded in legitimacy than any other's, and is going to and should be met with fierce resistance."[29]

[28] David R. Johnson & David G. Post, "And how shall the net be governed?: a meditation on the relative virtues of decentralized, emergent law", http://www.cli.org/ (17.11.2002).
[29] Johnson & Post, ibid.

b. Governance via International Treaties

Another possibility is to regulate and govern cyberspace by making international agreements which are to construct new and harmonized rules that are applicable in cyberspace. This way of solution has always been an answer to any issue which is of universal character. Especially this alternative, can help to ease the problems emerged from discrepancies between national statutes. In this way, the talent of users and operators to surf across physical boundaries might be responded by constituting a uniform law of cyberspace. Furthermore the problems aroused among nations can be eased.

There are also problems with this second model of governance. One of the problems is the disturbingly slow structure of an international treaty when compared to the almost day-to-day development of new horizons, new behaviors, conducts and governance issues, on the net. The information systems continuously bears new questions that challenge our understandings and many of these questions need counter-actions. The second problem is that, it is not guarantee that any treaty process could gain agreement from all nations and those non-participating countries might come out as deficits. In other words, no treaty is likely to be successful in imposing any predetermined rules on the cyberspace unless every nation whose fellows connect to the net participated in the treaty.[30]

c. Governance via International Organizations

The third alternative is to construct new international organizations which can attempt to create new principles and new ways of enforcing those rules. This model gives importance to the need for an international approach that will come out in order to govern cyberspace activity. The tremendous interconnectedness of Internet users, gathered with fears related to the feasibility of governance by nation states give way someone to advocate the development of international organisations on cyberspace standards and enforcement processes. The reason behind this idea can be found in the same style that the international seas, continent Antarctica or the outer space are handled as international spaces, the legal rules of which are embedded in the principles of international law.[31]

"Such an international organisation, independent from any national government and whose task is solely to establish and enforce basic rules for the cyberspace. This model would probably avoid some of the problems identified in the prementioned alternatives, since it would not be liable to a specified terrain or need to ask the views of related governments on a peculiar topic. However, the sensitiveness of this model is that, such an organisation would not easily find himself powerful enough to govern and set the rules for the cyberspace.

[30] Mc Neill, ibid.
[31] ibid.

Another point is the weakness of this model for being captured by factions. Indeed, such an organization will easily be invaded with factions of different political ideas and this nature of organization will endanger its benefits and make it impossible to control forthcomings."[32]

d. Self -Regulatory Approach

The fourth alternative is to create some necessary decentralized rules that come out as a collection of rules set forth by Internet users and system operators, deciding which de-facto rules to adopt, which filters to be valid and which users to be sign on, and with which other systems to connect and by users, regarding which personal filters to install and which systems to supervise.[33]

"Supporters of this regime who are sometimes called as being "anarchists" emphasize supposedly unique features of the cyberspace, such as its globality, decentralized, and non-hierarchical architecture, which make it extremely difficult and probably illegitimate for territorially based governments to enforce either their traditional legal rules or Internet specific rules. They treat those features of cyberspace being as positive since nation-states are incapable to regulate it. They believe dubiously, forms of self-regulation are the only possible or perhaps the best means of governing cyberspace and state-based law is not able, or is not best suited for the regulation of cyberspace activities. They argue that the preconditions for successful governance of physical space, on which traditional state sovereignty rests, no longer apply to cyberspace. Hence, geographically-based state governance techniques cannot be effective in the governance of cyberspace, and indeed may not even be legitimately used. They tend to turn either to self-governance or to supranational institutions to provide the legal and coordinating bases under which cyberspace can flourish."[34]

This model depends on the features of the cyberspace that expresses itself as something more than a group of standards including message transmission, and reception. In fact, such a central and governmental body has never been elected to adopt a law stating that TCP/IP (Transport Control Protocol/Internet Protocol) is demanded to be used by those wishing to communicate in the cyberspace, or similarly, HTTP (Hyper Text Transfer Protocol) is called for to be used for the same purpose. In such a case, if anyone connects to the net takes and sends out packets of data that is in conformity with the protocol, his messages can be heard by others who use the same protocol. All of them are free to reject accepting or following the standard and to perform some other protocols. In such cases, they will communicate only to those who uses the same protocol.[35]

"There are some important assets which this approach offer us. First, due to its non-governmental

[32] Johnson & Post, ibid.
[33] ibid.
[34] Mc Neill, ibid.
[35] Johnson & Post, ibid.

structure, it provides widest protection for freedom of expression and other fundamental rights. There is also a benefit offered by this model that outstands as to be less intrusive when compared with previous alternatives. Indeed, preceding models inevitably invite intrusion of both national or international organizations and this consequences a real negative impact on the civil liberties and fundamental rights. Furthermore, because of its flexible and easy to correspond features, this model fits best in case of any technological novelty that risks the course of communication. Furthermore, self-governance may be desirable because it is more efficient, because it makes sense to have rules for the community included in the self-governance regime which are different from or which are enforced in different ways from the surrounding community, because it is impractical to apply the rules of the surrounding community, or because compliance with the norms of the community is higher when members of the sub-community participate in self-governance. Partisans of self-regulation do not, however, necessarily exclude any role for territorially-based governing institutions. There is an acceptance that there are limits on the capacity of self-regulating institutions, especially where the actions of members of sub-communities have an impact on non-members of those communities. These external effects are worthy of regulation by more traditional means. Hence, what is needed is a vision of governance which acknowledges the complex mixture of state, business, technical, and citizen forces. While the private sector will be a driving force in the development of the information society, governments also must be involved to protect public interests."[36]

Although this model provides good benefits to cyberspace governers, it also has some deficits. For example, the system does not bring any mechanisms to define, illustrate, and punish intolerable activities. Furthermore, one can hardly believe that such an emergent system will move in conformance with the principles we know as "law". Origin of those standards of behavior are "ethics" and "custom" instead of something we know as "law". However, public interest and protection regarding cybercrimes have always required something stronger than that. These tools can either be the chances to exert physical force in the outer world, or to put perpetrators in real jails. This is the strongest objection to this model pointing the reality such that behaviours on the cyberspace might have unbearable real-world impacts on people who have not agreed or even not aware of those rules.[37]

3. Inference

Although, Internet has reached a huge number of users in a very short period of time, today, there are no pure and efficient methods for administering and governing it. This deficiency has driven many people to look for ways to manage it. People first of all made their comments on whether cyber-world should be regulated or not.

[36] Mc Neill, ibid.
[37] Johnson & Post, ibid.

Consequently, there has been reached a conciliation, accepting cyberspace is not a "lawless" place and it should be exposed to some sort of regulations. However, there are still difficulties in deciding and postulating the necessary laws. Those who accept cyberspace as solely a separate and indifferent "place" are mistaken. They do not concentrate on the fact that activities taking place in cyberspace might have genuine impacts and for this reason, it is needless to develop a separate law of cyberspace.[38]

None of the methods we mentioned above are merely able to resolve the problem of cyberspace governance and these governance disputes will probably not be resolved overnight. In today's society of information new and especially legal approaches must consider the peculiarities of information as a new value but also as a new potential of risk. The problems of cyberspace governance and cybercrime treatment can only be overcome by a combination of multi-layered international initiatives. These actions should involve some other tools to be successful in fight against cybercrimes. These tools are technological and organizational measures, education, industry and the law.[39]

Because of its unrestricted, borderless and spherical structure, it is inevitable that any unique national regulations or efforts towards governing cyberspace will result in failure. For this reason, we believe, any national legislation must be dependent or and in relation to or move in conformity with international initiatives.

We believe, the best approach to govern cyberspace is to follow a multi-layered approach, including simultaneously four alternatives we mentioned above. As a matter of fact, there has been made some recent studies by main actors in the international forum such as United Nations, G-8, OECD, Council of Europe and European Union. In the following subtitle we will try to analyze recent efforts made by those international organizations.

III. CONCLUSION

The growth of the Internet and the proliferation of computer technology has offered new chances for those who would associate with illegal activities. The course of technology and online communication facilities has not only produced an outstanding increase in the incidence of criminal activities, but also resulted in the emergence of what appear to be some new varieties of criminal activity. The increase in the incidence of criminal activity as well as the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.

Because cybercrimes are frequently in multidimensional and transnational feature, perpetrators may take advantage of gaps in the present regulations to avoid identification and/or prosecution. It is therefore of great importance that every legal system take

[38] Wall & Walker & Akdeniz, ibid, p. 16 ; Mc Neill, ibid.
[39] Sieber, ibid. p. 202.

measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes.

So far, the challenge of cyberthreat have been treated in many different levels, deviating from national legislations to self-regulatory regimes and international approaches. All those efforts showed that just one of the levels would be too far away from providing a remedy and therefore a joint policy should be developed.

We believe, due to its supranational character, treatment of cyberworld is fit best through international conventions aiming harmonisation in this field which is strongly supported by national legislations. However, we should accept the difficulties in the harmonisation of national penal laws due to the misbelief accepting it still a core matter of state sovereignty and therefore proved to be more resistant to international harmonisation.

This extract concludes that law enforcement officials can not effectively prosecute cybercriminals unless they have the necessary legal tools to do so and the struggle against cybercrimes should be supplemented by "law". As a matter of fact, this leads us to the notion that cyberspace is not a "lawless" place and should never remain so and the legal tools for fight with cybercrimes should comprise of an arsenal of well-defined cybercrime offenses for use in prosecuting cybercriminals and some efficient procedural rules governing evidence-gathering and investigation.

The United Kingdom's Counter Terrorism Strategy

Maj. Julian CHARVAT*

The government of the United Kingdom launched and updated strategy for countering International Terrorism in March 2009. Titled Pursue Prevent Protect Prepare, the strategy is commonly referred to as CONTEST II (COuNter TErrorism STrategy). These papers will pré'8ecis the strategy and its reasoning and develop assessment and conclusions. All views expressed are those of the author and do not necessarily reflect those of HMG or the UK MOD, Crown Copyright is acknowledged throughout.

Prime Minister Gordon Brown recognises the first priority of the Government is to ensure the security and safety of the nation and all members of the public.[1] In the current climate of International Terrorism, the United Kingdom has suffered many attacks or attempted attacks from Al-Qa'ida or associated terrorist groups and has also a threat of terrorism from dissident groups in Northern Ireland. International Terrorism has targeted the United Kingdom with foreign terrorists and also by radicalising elements of British society and recruiting the extreme elements of these as terrorist activists. It therefore gives the United Kingdom's security services the task of finding and disrupting potential attacks on the country and its interests both at home and overseas while protecting the freedoms the people enjoy.[2]

The aim of the CONTEST is "To reduce the risk to the UK and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence".[3]

The strategy recognises the key commitments to human rights and the rule of law when combating terrorism. Although terrorist attacks abide by no rules and will target innocent civilians, the response to these attacks and the disruption of them must be met with legal and moral means otherwise they may reinforce the wrong message. The United Kingdom's principles make clear the need to address the causes as well as the symptoms of terrorism and emphasise the need for partnerships at home and overseas to deliver CONTEST successfully.

There is no internationally agreed definition of terrorism; however the Untied Kingdom gives its interpretation of terrorism in the Terrorism Act 2000 as:

Interpretation

(1) In this Act "terrorism" means the use or threat of action where—

(a) the action falls within subsection (2),

(b) the use or threat is designed to influence the government or to intimidate the public or a section of the public, and

(c) the use or threat is made for the purpose of advancing a political, religious or ideological cause.

(2) Action falls within this subsection if it—

*UK A, Course Director, COE-DAT

[1] CONTEST II Forward by the Rt Hon Gordon Brown MP, Prime Minister.

[2] The Rt Hon Jacqui Smith, Home Secretary in her forward to the CONTEST.

[3] Pursue Prevent Protect Prepare, The United Kingdom's strategy for countering international terrorism (CONTEST) pp 6

(a) involves serious violence against a person,

(b)involves serious damage to property,

(c) endangers a person's life, other than that of the person committing the action,

(d) creates a serious risk to the health or safety of the public or a section of the public, or

(e) is designed seriously to interfere with or seriously to disrupt an electronic system.

(3) The use or threat of action falling within subsection (2) which involves the use of firearms or explosives is terrorism whether or not subsection (1)(b) is satisfied.

(4) In this section—

(a) "action" includes action outside the United Kingdom,

(b) a reference to any person or to property is a reference to any person, or to property, wherever situated,

(c) a reference to the public includes a reference to the public of a country other than the United Kingdom, and

(d) "the government" means the government of the United Kingdom, of a Part of the United Kingdom or of a country other than the United Kingdom.

(5) In this Act a reference to action taken for the purposes of terrorism includes a reference to action taken for the benefit of a proscribed organisation.[4]

The CONTEST II has 4 main workstreams to counter and defeat the terrorist threat to the United Kingdom which are known as Pursue, Prevent, Protect and Prepare. These are designed to form a comprehensive approach to the issue of terrorism and to tackle to motivations and factors that cause it. As terrorism has the purpose of advancing a political, religious or ideological cause there is a opportunity to defeat the idea of terrorism and address the root causes at a conceptual level through communication.

The United Kingdom assesses the main threat to come from four main sources, the Al-Qa'ida leadership and their immediate associates, located mainly on the Pakistan/Afghanistan border; terrorist groups affiliated to Al-Qa'ida in North Africa, the Arabian Peninsular, Iraq and Yemen; 'self-starting' networks or even lose individuals, motivated by an ideology similar to that of Al-Qa'ida, but with no connection to that organization; and terrorist groups that follow a broadly similar ideology to Al-Qa'ida but which have their own identity and regional agenda.[5] Although these four elements are seen as the primary threat today and in the future, the CONTEST II is designed to tackle any terrorist threat to the United Kingdom.

International Terrorism and the UK

The threat from International Terrorism is not a new experience for the United Kingdom. Since the end of the Second World War the UK and its interests have suffered

4 Terrorism Act 2000 Part 1 Section 1
5 CONTEST II Sect 0.10 pp9

terrorist attacks from Zionist terrorist in the British Mandate of Palestine and by nationalist terrorists in Cyprus.[6] The Troubles in Northern Ireland saw terrorist activity in the Province and the UK mainland from 1969 until 1998 with some attacks by small dissident breakaway groups continuing in 2009. It is however assessed that the international terrorist networks pose the greatest threat to the United Kingdom's security from both foreign and domestically recruited terrorist activists.

Since the 1990's the United Kingdom has had Al Qa'ida operatives and associates operating from its territory. Some British based groups encouraged participation in violence overseas in areas such as Bosnia and Chechnya. Some UK based individuals began links with Al Qa'ida and some pro Al Qa'ida propagandists entered the United Kingdom and began to establish bases from which they intended to recruit and radicalize potential supporters. In 2000 an attack was planned in Birmingham but it was disrupted by the police and security services. It was initiated by individuals sympathetic to Al Qa'ida, one of who had trained in Afghanistan.[7] Since 2001 the security services in the United Kingdom have successfully disrupted over a dozen attempted terrorist plots and the attacks on the London transport network in July, both the deadly 7th of July and unsuccessful 21 July plot, which involved people linked or part of Al Qa'ida.[8]

It is assessed that there are four main factors that have led to the threat of international terrorism and networks against the United Kingdom; conflict and instability, ideology, technology, and radicalization.

Over the past two decades many areas that have been in conflict have become focal areas for terrorist groups. The terrorist participation in these conflicts has given them operational experience and has given them access to develop the technology of terrorism, notably the IED threat. These conflicts have also been used to gain support both locally and internationally for the terrorist organization as it will often purport as being or offering the only viable solution to that conflict or situation. Failed states have also been exploited by terrorists, as they are often unable to protect their population and do not have the requisite capacity to deal with violent extremism.

The Al Qa'ida network has developed an ideology that draws on current conflict, historical events and misconceived religious aspirations that call for attacks on most western countries, including the United Kingdom. This ideology selectively draws on many philosophies and has tried to legitimise its terrorist activities and make it a religious duty to attack those Al Qa'ida targets.

Terrorist technology has had an impact on the threat to the United Kingdom in tow key areas, communications and tactics. The

[6] Cited in Hoffman
[7] CONTEST II 2.03
[8] CONTEST II pp. 26

increase of availability and access to the Internet has allowed Al Qa'ida to spread its extremist ideology and propaganda and reach those most susceptible to radicalization. Al Qa'ida has its own media organization, Al-Sahab, which helps it capitalise on promoting its message.[9] There are also new opportunities for international terrorists to engage with sympathisers and prospective recruits on line and to use the Internet as a medium for fundraising.

Radicalization is the process by which people come to support terrorism and violent extremism and, in some cases, then to participate in terrorist groups. Radicalization is the fourth key driver of contemporary international terrorism and in one sense the most important: none of the other strategic factors identified would enable terrorism unless people were also prepared to support it.[10] There are some factors that make the United Kingdom a potential target for those radicalised by the Al Qa'ida philosophy. There are many people who believe that the United Kingdom has caused conflict or failure in the Islamic world, or done too little to prevent it. This view has not in itself radicalized them but has made them more susceptible to the ideas promoted by Al Qa'ida. It is important to understand the causes of radicalisation to ensure that policy and action by the security forces and governments of countries do not unintentionally marginalise people or confirm the propaganda espoused by Al Qa'ida or indeed any other terrorist organization.

The Strategy

The strategy for countering international terrorism is based on a fundamental set of principles which will form the bedrock of the concept throughout. It is important to maintain human rights and the observance of this fundamental principle is at the heart of CONTEST II. Terrorism is a criminal act, it is therefore considered that the rule of law is maintained in all terrorist investigations and activities to ensure the legitimacy of any action taken and due process of those involved in terrorist activity. The CONTEST II is based around freedom, tolerance and opportunity for all with the aim of allowing all people to go about lawful and legitimate daily business without fear or undue interference. It also requires open and legitimate government to ensure the validity of the strategy. CONTEST II operates under the criminal justice system and investigations into suspected terrorist activity will be led by the Home Office Police constabularies and supported by security and intelligence agencies. In order to met the principle that the strategy is to allow people to go about their daily business, proportionality is a key component, balancing the safety of the population and critical infrastructure with the ability to conduct normal daily life is an ethic that the strategy embraces.

The philosophy that terrorism cannot occur without some support is recognized as a significant issue and the United Kingdom Government considers policies that are not directly about counter-

[9] CONTEST II 5.14
[10] CONTEST II 5.18

terrorism will be cognisant of the strategy. Reducing support for terrorism and violent extremism and preventing people becoming terrorists are vital.[11]

Pursue

Pursue is one of the four workstreams of the CONTEST II. Pursue is the workstream that aims to stop terrorist attacks by disrupting and prosecuting suspected terrorist under the law. This allows the Crown Prosecution Service to repeatedly bring successful cases, between 2001 and 2008 almost 200 people were successfully convicted of terrorist-related offences.[12] Intelligence drives the pursue workstream, as terrorist are secretive by the very nature of their activity, covert intelligence is often used which are led by the security services working closely with the police. The United Kingdom has greatly enhanced its intelligence capability in recent years to meet the increased threat of international terrorism. The Security service doubled between 2001 and 2008 and the number of police dedicated to counter-terrorism work has grown by over 70%.[60] The intelligence capability of the Prison Service has been enhances where they are dealing with prisoners suspected or convicted of terrorist related offences and the Border Agency has a greater intelligence capability than before. The collaboration among different intelligence agencies has been an area of improvement, the Joint Terrorism Analysis Centre was established in 2003 and joint operations and exchanges of staff have help the United Kingdom's agencies make collaborative working the normal practice. Likewise the counter-terrorism structure of the police and other agencies has been comprehensively reviewed and improved to give greater coverage and cooperation among all forces engaged in the Pursue workstream. This has also been extended to create partnerships overseas where there may be a threat to the United Kingdom and its interests, these have included intelligence exchanges and training.

The pursuit of terrorist utilises a wide range of lawful powers. Between 2001 and March 2008 there were over 1450 arrests which were terrorist related, with around 10% of these resulting in alternative action such as through immigration powers.[14] As, by its very nature, a significant threat from international terrorism is posed by foreign nationals or naturalised citizens, the United Kingdom has developed measures to reduce this threat. The Home Secretary has the power to exclude foreign nationals from entering the United Kingdom under certain circumstances. She also may revoke British Citizenship provided it would not leave that person stateless or if it has been obtained by fraud. Between July 2005 and the end of 2008 153 people have been excluded from entry to the United Kingdom on national security grounds and a further 87 for unacceptable

[11] CONTEST II 7.03
[12] CONTEST II 8.01
[13] CONTEST II 8.04
[14] CONTEST II 8.16

behaviour, three notices for the revocation of citizenship have been served.[15]

Under the Pursue workstream the United kingdom has build a comprehensive strategy to disrupt terrorism, including terrorist finances which can be frozen if the assets are found to support proscribed terrorist organizations. This workstream aims to look at all aspects of terrorism and secure the safety of the United Kingdom by catching those planning any terrorist activity and preventing attacks through intelligence let legal methods. It also concentrates on capacity building in areas of the world that might have international terrorism operating there.

Prevent

The Prevent workstream is the United Kingdom's approach to tackle the causes of radicalisation through a better understanding of them. It has five main objectives;

1. to challenge the ideology behind violent extremism and support mainstream voices,
2. disrupt those who promote violent extremism and support the places where they operate,
3. support individuals who are vulnerable to recruitment, or have already been recruited by violent extremism,
4. increase the resilience of communities to violent extremism, and
5. to address the grievances which ideologues are exploiting.[16]

The Prevent strategy looks at forming partnerships with communities and representative groups to target and address the reasons people may be drawn to extreme or Al Qa'ida style views. It has brought together leaders and scholars to promote the mainstream views and to challenge ideologues within the community. It is understood that there are perceived grievances within some communities in the United Kingdom over foreign policy, specifically the United Kingdom's involvement in Iraq and Afghanistan as well as social and political problems at home. This is being tackled by the Prevent workstream to counter the extremist version of events. In partnership with faith and community leaders the mainstream voice is being raised through a series of government funded workshops, road shows and other educational means. Incorporating such partnerships with those mainstream leaders of the communities most likely to be vulnerable to extremism is vital. This is conducted at both local and national levels.

The role of the police is an important facet of Prevent. Community police initiatives have been established to tackle individuals who are promoting violence and involved in recruiting for extremist organizations and target the areas in which they operate. In 2008 some 300 staff were ring fenced to work on this initiative. There is also an important international dimension to Prevent. The threat of international terrorism

[15] CONTEST 8.19-8.22
[16] CONTEST II Part 2 Sect 9 Summary

can come from foreign nationals and British citizens who have attended radicalization and training camps overseas. The Government of the United Kingdom works with foreign governments in areas where such camps do or may exist as well as diaspora communities in the United Kingdom to help understand and resolve issues. Various initiatives have been introduced to challenge the ideology behind violent extremism which works alongside scholars and faith groups to develop positive alternatives to extremist ideologies. These are also at regional, local as well as national levels to engage those vulnerable to extremism.

Vulnerability occurs for many reasons, it is not just an attraction to a certain ideology but social, family and community concerns or pressure may compel people towards such a view. Many new programmes have been introduced to address these and provide accurate information about the United Kingdom's foreign policy when it is grossly misrepresented by ideologues.

Protect

While the Pursue and Prevent workstreams tackle the concept of violent extremism and those who perpetrate it the Protect workstream reduces the vulnerability of the United Kingdom and its interests overseas to terrorist attack. This workstream will make it much harder for terrorists to gain entry into the United Kingdom and then attack the targets experience has shown them to prefer.[17] There are four key areas the United Kingdom is strengthening to protect against the risk of terrorist attack, namely:

1. the critical national infrastructure,
2. crowded places,
3. the transport system, and
4. the United Kingdom's borders.

Critical Infrastructure is a key target for terrorism with the intent to disrupt daily life and cause casualties. The Protect workstream has been divided into 9 key areas, communications, emergency services, energy, finance, food, government, health, transport and water. In 2007 the United Kingdom set up the Centre for Protection of National Infrastructure to provide integrated security advice across the national infrastructure on physical, personal and electronic security. This initiative incorporates security for state and private infrastructure and has evaluated over 200 security products since coming into being.

As the threat of international terrorism includes the risk of mass casualties, crowded places have been assessed as a potential target. To reduce the risk to such places the United Kingdom has established the National Counter Terrorism Security Office to provide advice and assistance to those responsible for crowded places and the storage of chemical, radiological, biological and explosive materials. Nationwide there are over 250 advisers available for support. Projects have included sports stadia, shopping centres and city centre clubs and bars. A National Barrier

[17] CONTEST II 10.01

Asset has also been established to provide temporary protection to key events from the risk of vehicle bourn suicide attacks.

As July 2005 highlighted, the transport system is a potential target for international terrorists. Transport networks are critical national infrastructure and also crowded places. Aviation security is the most mature of the initiatives and has been improved over recent years. In flight and ground security has been revitalised to meet the ever changing threats international terrorism poses to it. Measures to strengthen flight doors, restrict the carrying of liquids and provide an in-flight armed policing capability have been brought in.[18] since 2003 there has been a multi-agency threat assessment to provide critical security measure advice to all key stakeholders in airports. This has also included partnerships and advice for UK airlines operating on international flights.

The United Kingdom has helped develop many international initiatives for Maritime security as it has a developed programme before 9/11 and was at the forefront of such initiatives. It was a lead for the International Maritime Organization in the development of the International Ship and Port Facility Security Code. The United Kingdom's rail and underground systems have also been subject to new security innovations. Although both systems had a heightened security status as a response to the threat of Provisional IRA attacks in the 1970s and 1980s, further security has been developed. The use of explosive detection dogs to screen passengers and baggage has proven effective and works in the subterranean environment of the underground.

Initiatives have also been introduced in the United Kingdom's border policies to reduce the possibility of entry into the country by suspected terrorists. The police and border agencies work closely together and have a watch-list system for goods or persons of interest who may attempt to enter the United Kingdom, this included suspects for serious and organized crime as well as terrorism or terrorist related activities. An e-border programme has been developed to allow passenger manifests to be screened prior to arrival in the United Kingdom and to alert the authorities of any persons of interest attempting to enter the country. The United Kingdom introduced a biometric visa system in 2007 requiring the biometric information from those requiring a visa to enter the country.

New developments in the screening for Chemical, Biological, Radiological, Nuclear and Explosive materiel entering the United Kingdom have also been introduces. This has included security advice for those working with such materiel to reduce their personal risk.

Prepare

While every effort is made to Prevent a terrorist attack it is understood that should one occur the country must be able to deal

[17] CONTEST II 10.01
[18] CONTEST II 10.10

with it and to mitigate the effects of it. Preparations must be in place to manage the attack scene itself, support the victims of the attack and to get the critical infrastructure affected up and running as soon as possible. This planning will also cope with non-terrorist related incidents. The main objectives of the Prepare workstream are to ensure that the right capabilities are in place, there is swift recovery and central, regional and local crisis management structures are appropriately equipped, competent and trained. The United Kingdom has developed a comprehensive crisis management system that has learned from several non-terrorist incidents such as the 2001 Foot and Mouth crisis as well as some terrorist attacks such as the London Transport attacks in July 2005. The approach encompasses civil authorities, the police and the Ministry of Defence who can provide specialist and logistic support in many areas. Improvements have been made in the areas of communication among responders and victim support in the wake of the July 2005 attacks.

The Prepare workstream will base its assumptions on the National Risk Assessment which set out the assessed risks for a five year period and the National Resilience Planning Assumptions which set out the potential consequences of these risks.[19] Regular reviews of the plans and realistic training ensures that all agencies can cooperate to deliver the appropriate response in a timely manner for any emergency situation.

The government of the United Kingdom works closely with the private sector to maximise cooperation and security among all involved in the mitigation of an emergency. It has also developed key initiatives in the protection and preparation for any event involving CBRNE materials.

Communication

It is understood that the messages and language used in relation to terrorism have a great effect on it. It is vital that the audience is understood and appropriate regard is made to cultural and historical sensibilities to ensure that the language of any communication is accurate and not subject to misinterpretation. Great effort has been made to ensure that communications made by the United Kingdom do not exasperate any situation or cause division among different communities at home and abroad. The communication strategy is also a key tool in defeating the propaganda and communications from international terrorists by exposing inaccuracy and fabrication in them.

Conclusions

There is a real and current threat to the United Kingdom from international terrorism. This threat occurs for a variety of reasons and a comprehensive approach has been developed to counter this. The strategy has been developed within the principles and values of the United Kingdom as a liberal democracy and is grounded in a

[19] CONTEST II 11.18

set of core values. The Government of the United Kingdom has committed to include human rights, the rule of law, open and accountable government, justice, freedom and opportunity for all. The strategy recognises the need to resolve issues at home and abroad where the United Kingdom's foreign policy may be misrepresented by international terrorist organizations.

The response to this threat is based on four main workstreams that aim to stop people supporting terrorism or becoming terrorists, stopping terrorist attacks and if they do occur to mitigate them by a quick and manages response and recovery.

References

[1] Pursue Prevent Protect Prepare – The United Kingdom's Strategy for Countering International Terrorism, Norwich, TSO, March 2009

[2] Hoffman, Bruce: Inside Terrorism, New York, Columbia Press, 2006

Acknoledgement: This article draws extensively from the HM Government publication Pursue Prevent Protect Prepare – The United Kingdom's Strategy for Countering International Terrorism, Norwich, TSO, March 2009. It has been extensively quoted under Crown Copyright beyond the direct references used. All views expressed are those of the author and do not necessarily represent the UK Government, MOD, NATO or COE DAT.

Strategic Communication For Combating Terrorism Workshop

Maj. Aykut ÖNCÜ*
Maj. Troy BUCHER**

On 12-13 May 2009, COE–DAT in Ankara conducted a workshop on "Strategic Communication for Combating Terrorism." The aim of the workshop was to bring together academics, experts, and military professionals to improve concepts for using strategic communications in combating terrorism within NATO. This paper summarizes the content of the various lectures and the conclusions drawn from those lectures. The full workshop will be published in book format in late 2009.

This workshop 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, and a participatory audience from the NATO Countries, to bear on the use of strategic communications for countering terrorism.

Significant reactions and comments based directly on the concrete experiences of those parts of the world enabled the creation of an environment of dialogue, increased transparency, and mutual confidence. In this respect, the Centre was seeking to reach a common understanding of the framework of this subject, and to determine common themes that may form the guide for future policy development in respect to the subject. COE-DAT plans to remain involved with SHAPE Strategic Communications through both continued participation in their working group and by providing DAT expertise and input to future Strategic Communications policy development.

The workshop itself brought together 30 participants from eight NATO Countries and 15 academicians and experts on terrorism. The workshop itself consisted of four panels. Each panel contained 3-4 presentations that lasted 30-45 minutes including the question and answers period. The last period of each day contained a one-hour panel discussion among the speakers and participants.

* TUR A, Concept Officer, COE-DAT
** USA A, OPS Officer, COE-DAT

1. CONCLUSIONS

Independent scholars, consultants, and military personnel provided the lectures for the COE-DAT workshop on Strategic Communication for Combating Terrorism. In both the lectures and continued panel discussion, there were exhibited a number of very strong themes, each of which was common to several of the lectures. These themes, captured by Dr. Corman of Arizona State University, are listed below.

a. Engagement

The strongest theme had to do with engagement. Speakers stressed the importance of increased engagement with strategically important audiences and communication channels. The four aspects of this theme were:

- The need to view strategic communication as a two way process of communication. This contradicts the traditional view that communication is a one-way process of transmission and highlights the importance of strategic listening and dialog.
- The importance of personal contact between NATO personnel and target audiences and populations, so as to better understand their views, interpretations, and culture.
- The need for NATO communicators to improve familiarity and engagement with the 'New Media.'
- The critical factor of engagement with policy formulation, treating policy as an aspect of strategic communication rather than the traditional system treats strategic communication as a way to "sell" policy.

b. Media Landscape

Many speakers addressed the radical changes in the media landscape over the last decade that have changed the role of the traditional media and created many new types of media. These changes represent an increase in the overall importance of the media and a growing need for engagement with the full spectrum of media channels. Adapting to the new landscape is critical to the success of NATO strategic communication efforts.

c. Complexity

Numerous speakers noted the revolutionary increase in the complexity of 21st Century strategic communication systems due to factors like globalization and the burgeoning media landscape already mentioned. These changes not only make the strategic communication system more complicated but provide opponents with the ability to adopt more complex and agile organizational forms.

d. Control

In the past best strategic communication practices were concerned with control of messages. But new realities create a system with levels of uncertainty that make control impossible. Treating the 21st century systems as simple and controllable, when they are not, leads to negative outcomes and strategic communication failures. This presents a significant challenge for NATO communicators, because their practices and systems were developed in the last century, when

control-based communication was more practical, and are proving slow to change.

e. Narrative

Many speakers discussed the growing importance of narrative in strategic communication, which forms an important basis for interpretation of action by strategically important audiences. NATO nations are either doing a poor job of making their narratives clear, and are taking actions that contradict their narratives, thus undermining their credibility. At the same time they must do a better job of understanding and countering the narratives of their opponents.

f. Organizational Inertia

Inertia in the command systems of NATO and its member nations inhibits the change mandated by the five foregoing themes. While there is widespread agreement among theorists and operators that strategic communication practices must evolve to meet new 21st Century challenges, political and organizational structures of the status quo work against these changes, keeping the alliance in an underperforming posture that reproduces outdated practices. This is perhaps the keystone problem in NATO strategic communication, because it inhibits adaptation to the new realities discussed at the workshop.

2. SUMMARIES OF THE WORKSHOP PRESENTATIONS

a. Keynote Speech

Mr. Mark Laity, the Chief of Strategic Communications at SHAPE, gave the speech. The premise of the keynote speech was that "Terrorism is a form of strategic communications, no more, no less. It is not kinetic. It is in the head, working on the mind to make people afraid." The enemy practices information operations with kinetic effects while it is NATO forces that are playing 'catch-up.' We are behind. We need to not just think more, but differently. "Strategic Communication is about thinking differently."

"Look at the effects our opponents have had with Strategic Communications. Look at 9/11, it was Strategic Communications and classic information operations. As another example, an Afghanistan suicide bombing against a tribal leader was filmed from 3 angles, edited, and placed on YouTube and done in less than one day. They were not there to kill -they

were there to send a strategic message. Look at the Serena Hotel bombing. Within 30 seconds of the bombing the wire agencies had flash wire reports from the terrorists. Are we that good? No we are not."

NATO is "beginning to get into the game, but way behind." We have a directive from SHAPE, ACT 952, which is a move in the right direction. Now we need the people in SHAPE to know it and read it. "Policy may need to change to meet the needs of Strategic Communication," not vice versa. There is also now a vision statement that says Strategic Communications should be at the heart of all operations at all levels. Recognizing that, information policy is vital to success.

"Right now we spend too much time on coordination and process. We have now created organizations whose sum is less than the parts." He concludes by telling us that the way we currently conducting Strategic Communications is making us less effective. We need to look at this differently. "The enemy is fast, flexible, and more attuned to the cultures where they operate. We talk Narrative, but Narrative is where they beat us. We do messages and themes, and our opponents do Narrative and tap into cultures and religion."

b. Panel One - Overviews and Models of Strategic Communications

STRATEGIC COMMUNICATION: GENERAL OVERVIEW – Cdr. Steve Tatham

As Commander Tatham of the UK Defence Academy put it, we place "too much emphasis on communication versus the strategic, or strategy" in Strategic Communications. NATO needs to rethink the information effect and quite following a "linear push" fashion. "We are floundering on old ideas and simplicity" as he puts it. NATO needs to figure out its Strategy before it figures out the Communications part. We need to conduct better Target Audience Analysis and quite telling the enemy what we think they should hear from the message, instead of understanding what they actually hear from our words. As he puts it "we can't use the kinetic to win."

MARKETING APPROACH TO EARNING POPULAR SUPPORT – Dr. Todd Helmus

Dr. Todd Helmus of the Rand Corporation talked about conducting Strategic Communications using a marketing approach. Specifically, "Branding is a collection of perceptions in the mind." If there was a "military brand" for the cold war, it would be "force and might." "Is that suitable for todays operations?" he asks. Dr. Helmus goes on to tell us that the military needs a new brand, one that can be communicated at all levels and shape operations. It must provide a message that is instilled across all contact points. The military needs to follow the business industry and develop rules of interaction, not just rules of engagement. Like bad marketing, "Civil military leaders easily mistake population needs and wants." Instead the military tends to ignore customer satisfaction, does not manage expectations, and overpromises while under-delivering. To sum it up, if the

military had a brand name now it would be "occupier," that is what we are selling.

MODELS FOR STRATEGIC COMMUNICATION – COL(R) Ian Tunnicliffe

COL(R) Tunnicliffe of StratCom (Strategic Communications) Laboratories spoke on models of Strategic Communication. Currently one of our biggest problems is that no message is getting across because we do not have the credibility to reach our target audience. COL Tunnicliffe breaks it down, through various sales marketing examples, to our current process of Source, Message, Channel, and Audience. This is not effective if the target audience does not want the message and does not believe the source. For one, this does not define an objective first. It views the audience as just a receiver instead of taking into account their part in the message. It also does not take into account that the message is far less important than the source. Last, we need to constantly evaluate our effectiveness and adjust the model accordingly. The model should be Objective, Audience, Channel, Source, Message, and then Evaluation.

c. Panel Two - NATO and US Strategic Communication

NATO and US STRATEGIC COMMUNICATION ORGANIZATION – LTC Eric Campany

LTC Eric Campany, the Strategic Communications Planning Officer at SHAPE, gave a breakdown of current Strategic Communication organization in NATO. He explained that it was a new organization, minimally manned, and still developing its role in NATO command. The capabilities required by NATO to make Strategic Communications work are: Fused Information Analysis, Audience Analysis, Outreach (KLE, etc), Deployable Media Teams, and New Media (SHAPE will have a new media section, but what it will do is still undecided).

ACT has a huge role to play in developing Strategic Communications within HQ SHAPE, but currently there is a lack of agreement at the highest levels on the role of Strategic Communications. Right now, the StratCom section is developing policy, with ACO 95-2 Directive 15 Sep 08 being the only approved NATO document and it provides over-arching guidance for planning. Also the Strategic Communications organization at SHAPE utilizes a working group construct and a community of interest that works well in assisting in the development of policies and idea.

ISAF EXPERIENCE OF STRATEGIC COMMUNICATIONS – BG Martin Schellies

BG Martin Schellies of the German MoD spoke briefly about the Information Domain Challenges in the 21st Century, posing the question of 'Is Strategic Communication the solution?' As he put it, we already have the tools: PsyOps, Info Ops, Public Affairs, Public Diplomacy, but there is a lot of friction between the idea of Strategic Communication and Information Operations. BG Schellies explained his difficulties in ISAF as the Chief of Information Coordination Branch where these frictions to some extent limited capabilities. As BG Schellies stated the difficulty is that we need coordination across everything - partners, higher, government, etc. and that we will never be able to do this. However, we must never stop trying to achieve this and improve this. To paraphrase his conclusion, we need to come up with an overarching story/narrative/plan and we need vertical coordination within NATO and horizontal cooperation and coordination with partners at all levels.

US STRAT COM POLICY AND A MODEL FOR The 21st CENTURY – Dr. Steve Corman

Dr. Steve Corman from Arizona State University Hugh Downs School of Communications discussed how most of our Strategic Communications for the last 50 years has been based on a the SMRC model from the 1950's: Source, Message, Channel, and Receiver. Under this model the only things that prevented getting the right message across was if the message was not sent correctly, or there was interference in between. Under this model there is complete control by the sender and the receiver is not taken into account. This model was taught from the 60's through the 80's. This however does not fit in the modern world, is too simplistic, and does not work for a hostile audience. We have to stop stove piping messages, release control, and expect some failures. We also have to quite trying to segment audiences, the world is interconnected and media/messages are immediate and reach everyone.

d. Panel Three – Perception Management and Terrorism

THE ROLE OF PERCEPTION MANAGEMENT IN TERRORISM - Dr. Abdulkadir Çevik

Dr. Abdulkadir Çevik of Ankara University displayed an Islamic Crescent and asked what it meant. He said to him it was a positive symbol; however some may have suffered traumas and associate it with bad things. He discussed perception shaping and management and related this to terrorism. With the multimedia environment of the 21st Century it is hard to differentiate between reality and illusion. Humans are open to influence and some will distort reality for their own benefit. Dr. Çevik discussed the human psychology and the difference between reality and perception. External artificial factors affect this, such as media. Our perception is managed by

expectation; we often perceive what we expect to see. Every culture has a different expectation and way of perceiving events. Perception management is persuasion and skillful use of propaganda; this can be called a spin effect. Perceptions of individuals are frequently influenced by external forces and are modified to fit the desired attitudes. Terrorist organizations are large groups that use perception management techniques to modify the attitudes of its followers. Dr. Çevik gave a case study on ASALA and perception management and the Muslim experience post 9/11.

LANGUAGE AND COMMUNICATION STRATEGIES - Dr. Amy Zalman

Dr. Amy Zalman from Science Applications International presented about self-perception and its formation in self-image. The opinions of the civil population have always had an effect on war. The increase in media accessibility has amplified this. There has also been a change, in the 20th Century and before war was fought on a battlefield and only the population that was unfortunately in the way of the battle were directly caught up. In the 21st Century warfare is becoming more irregular and population, not geographic gain are the measure. This measure is not geographically based as Diaspora take the perception problem to a global level. Popular culture, imaging and the like play a role and make modern conflict complicated. Analysis has taken stock of perceptions and a macro-cultural dimension; communicators need to understand themselves and the perceptions of them as well as understanding the target audience and how they will perceive.

WINNING THE WAR OF IDEAS: EFFECTIVE LISTENING - Dr. Itamara Lochard

Dr. Itamara Lochard from the Fletcher School of Law and Diplomacy presented on the subject of effective listening. Her presentation is non-attributable.

HOW STRAT COMM CAN BE USED TO BREAK THE CYCLE OF VIOLENCE – Mr. Joshua Mora

Mr. Joshua Mora of the Behavioural Dynamics Institute of London used a model to explain his message, that of the stopping the spread of epidemic viruses. These will be biological and also social in nature and can be mapped, the spread of an influenza virus would likely follow flight routes and spread along them. Viral communications will have a very similar property. Mr Mora mapped out the model for a virus to spread and how the medical services will deal with it by targeting susceptible populations and tackling the disease. He related this to terrorist propaganda and communication to highlight how a message was spread and the junctures that it could be ‘tackled’. He drew that there would be those who would die of a disease and linked those to the radicals that no message could affect to those who were curable and therefore the main target for STRATCOM along with those not yet infected but who could be prevented from catching the disease.

e. Panel Four – Strategic Communication in Combating Terrorism

MEDIA COVERAGE OF TERRORIST INCIDENTS – Dr. Peter BUSCH

Dr. Peter Busch from King's College, London, looked briefly at classical terrorism reporting and studied the Mumbai attacks of 2008. He looked at how reporting was changing and considered the easily accessible new media such as Twitter and how this could change reporting of terrorist events. Over the last 10 years the scope of reporting has changed as new technologies allow more immediate news. Immediacy is a growing trend. There has also been a significant proliferation in news outlets on TV and the Internet. Citizen Journalists and "enemy" websites also provide an unregulated source of media output. Terror attacks bring these trends into sharp relief and give editors pressure to make instant decisions without time to check facts fully. Dr Busch looked at the Mumbai attacks and how they were reported. He considered the different media and the time and attention they devoted to the attacks and how this changed over a two-week period. It was noted how much coverage from local TV was used instead of the more expensive option of sending in foreign correspondents and crews. He also considered the effect of the social information site Twitter. This gives people the ability to publish short messages instantly via a mobile phone or computer. During the Mumbai attacks more than 1 message per second was sent with the word 'Mumbai' in the heading. Like all forms of unregulated reporting this gave some good and accurate information as well as some spurious inaccurate information and occasionally broke OPSEC. These new media have to be monitored and embraced as part of STRATCOM – if this is how people get and exchange information in the 21st Century it must be used to keep up to date.

SYNCHRONIZING INFORMATION: THE IMPORTANCE OF MEDIA/PERCEPTIONS – Matt Armstrong

Mr. Matt Armstrong of Armstrong Strategic Insight Groups began with the idea that there is currently a Now Media rather than a New Media. Many journalists and some PIOs are using media such as Twitter. Terrorism is an attempt to influence an adversary, power and influence equal control. Terrorism is an information tool and you no longer need a geographic proximity to influence people. Terrorists like an unstable environment and terrorism tried to destabilize. IEDs are not employed just to maim and kill, they influence TTPs and create propaganda. If a terrorist act is not known about it has little use. Kinetic action does matter in an information world. There is a struggle for minds, to influence the will to act. The access to, dissemination and distribution of information has increased. Precision and mass media almost give the feeling of being there but it is still reported word of mouth, a journalist on a satphone is still deciding what is said. It is now a global adventure, but one must not forget the message for the 'home' audience. Although the world is more on line there is still significance in TV, pamphlets and all traditional media. There is also a 'wealth of information but a poverty of attention. The perception and worldview is important. If people like terrorists put out information you must address it or somebody else will. Everyone is a communicator, actions change perceptions and how you act speaks. Soldiers may blog and communication must be internal as well as external. Mr. Armstrong used a video to show how information can build from nothing to a full article on Wikipedia in a very short time. Perhaps the Twitter effect is replacing the CNN effect in communications.

CRY TERROR AND LET SLIP THE MEDIA DOGS – CAPT (R) Randall Bowdish

CAPT (R) Randall Bowdish of the University of Nebraska presented on both ethical questions involving in the media and that the media's messages had a physical effect on the audience. The terrorist perspective is an army of a few facing a state and is therefore asymmetric. Terrorism is a tactical act against a strategic audience. Messages my have small lethality but a big effect and the media is the fulcrum for this. Free press is the soft underbelly of democracy, journalists provide free and accurate information to allow democratic choice and safeguard against tyranny. Terrorists can exploit this. Terrorism ignores the accepted limits in moral information. Terrorism will need to be newsworthy; it must reach a certain threshold to have an effect. It must also be meaningful enough for the press to report. There is an event and a message in terrorism. The terrorist has to look at the effect on the target. Reports of terrorism can do cognitive harm to the public. It can cause anxiety and stress to those not physically affected. Can this harm be stopped? An academic research model can be applied. In

the 1950s there was no limit on psychological experiments involving humans and this was found to possibly cause harm. Now such tests require certification. There can be tension between the free press and the government. If limits are put on the press it may be hard to retract them and be the first step to tyranny. Perhaps the answer is to only allow journalists who have had ethical training to have access to official sources.

THE IMPORTANCE OF THE INFORMATION FACTOR IN COIN OPS - Col Dirk Brodersen

Col Brodersen of the German Bundeswehr looked at a tactical level. Land forces are only 1 element of an orchestrated COIN (Counterinsurgency) campaign, it is a joint environment including non-military agencies such as NGOs. There is a campaign theme; tactical activities may vary in precedence over time. There will be tactical tasks in a tactical toolbox and COIN is an element in a stabilization campaign. Irregular forces may be under many names, the choice of name is part of the information campaign. Insurgents are smaller but may chose limited battle and accept losses. Insurgents may be a diverse force and not all violent. Our information can affect these, either by reinforcing their views or pushing them away from the insurgency. However the message target is the population and not the insurgent. Operations send a message in the information environment. An event can hit many audiences in many ways. Terrorists will seek to make the population lose faith in the military and government. There needs to be a wedge driven between the population and the insurgents. The key is finding a leverage point. There is a holistic estimate of the situation, to look in detail at the adversary. An organized crime group may be benign or pro the security forces if it is left alone, but may become pro-insurgency if it is affected. The course of action (COA) must be draw after looking at all factors and their consequences. Knowledge is the key to make decisions. COIN is not in isolation by LAND component, it is part of a much wider campaign. Everything revolves around the population. Effort must be put into INFOPS as well as tactical ops.

COE-DAT Activities

1 Brig. Gen. David ECCLES CBE, UK National Military Representative (UKNMR) at SHAPE visited COE-DAT on 16 Jul 2009.

2 A delegation headed by the Commander of Maritime Interdiction Operational Training Centre; RADM (L) Mazarakis Ainian KONSTANTINOS on 18 August 2009.

3 The Chief of Intelligence of USEUCOM, Brig Gen. Greg C. POTTER, visited COE-DAT on 18 August 2009.

4 A delegation from Sweden headed by Col.Lennart DANIELSSON, Deputy Chief of International Relations Department of Swedish General Staff visited COE-DAT on 24 September 2009.

Future Activities

1 COE-DAT is organizing an Advanced Training Team (ATC) about "Cyber Terrorism" on 12-16 October 2009 in Moldova. The course intends to discuss the history of internet, terrorist use of internet, developing worldwide web, legal issues of cyber terrorism and cyber attacks against NATO.

2 COE-DAT is going to conduct its third course on "Terrorism and Media" on 02-06 November 2009 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.

3 COE-DAT is going to carry out a "WMD Terrorism" course on 09-13 November 2009 in Ankara/Turkey. The course intends to analyze past, present and future of the proliferation of the Weapons of Mass Destruction (WMD), the means and methods both for preventing terrorist attacks with WMD and also means and methods for the first responders and the legal aspects of defence against WMD terrorism.

4 COE-DAT is going to hold a workshop on "Homeland Security Organization in DAT" on 19-20 November 2009. The workshop aims to provide a forum for officers and selected appropriate civilians from NATO, MD, PfP and other countries to discuss homeland defence regarding terrorism.

5 COE-DAT is organizing an Advanced Training Team (ATC) about "Defence Against Terrorism" on 03-07 January 2010 in Jordan. The course intends to analyze the terrorist threat with different dimensions and examine counter-terrorism strategies in detail.

6 COE-DAT is going to conduct the third "Global Terrorism and International Cooperation Symposium" on 15-16 March 2010 in Ankara/Turkey. The symposium aims to provide a forum for exchange of information and expertise among the pace-loving nations in defence against terrorism. The symposium intends to bring together world's most renowned scholars and practioners with unique expertise as well as the distinguished decision makers including heads of states, governments and ministers.

COE-DAT Publication

Defence Against Terrorism Review(DATR)
Centre of Excellence Defence Against Terrorism (COE-DAT)
Vol.2, No.1, Spring 2009

The third issue of Defence Against Terrorism Review (DATR) has been published. The new issue is composed of invaluable articles by distinguished scholars. COE-DAT appreciates their contribution and is proud to share it with its readers.

The Defence Against Terrorism Review (DATR) is a refereed, interdisciplinary, biannual journal, publishing in-depth analysis of the complex issue of terrorism in a changing and globalised security environment. It includes political, legal, sociological, economic, and psychological approaches to the terrorism predicament. DATR intends to reach academics as well as practitioners and aims to publish theoretical as well as policy papers. It also encourages contributions from different cultural perspectives.

The Defence Against Terrorism Review (DATR), first published in the Spring of 2008, is now one year old. DATR presents with great pride its third issue Spring 2009 in which our readership will again find, we hope, a collection of very valuable articles on extremely interesting subjects by distinguished scholars, professionals and experts from around the world. It goes without saying that terrorism has many faces and DATR addresses in this issue only a few of the types of terrorism that the world community is facing.

In his article on the threat posed by the weapons of mass destruction (WMD), Guy Roberts discusses the important and dangerous challenges NATO faces and he highlights the complex nature of NATO's work in trying to create a 'holistic' deterrence posture. The author also makes some suggestions towards maintaining NATO's ability to combat WMD terrorism.

Relations between staunch allies Pakistan and the United Stated have since September 11 attacks been deteriorated due to the severe criticisms of the American administration about the reluctance of Pakistani authorities to give all the support they needed in their fight against Al Qaeda, which uses Afghanistan and Pakistan as a sanctuary. Moeed Yusuf argues that once Pakistan's own threat perception and self-defined regional objectives are held constant, it becomes entirely rational for it to avoid complementing the US objectives wholeheartedly. He, therefore, suggests that the United States should

change Islamabad's cost-benefit equation by altering the incentive payoffs rather than hoping that the moral undertones of the discourse would somehow lead it to oblige fully.

With the advances in IT technologies, issues pertaining to terrorism and the fight against it are taken to a new and more complex level, namely the cyberspace. Gilbert Ramsay argues that strategies for offsetting the advantages that terrorists may have in the cyberspace do exist. The author suggests that by recognizing the limitations of the Internet as a tool for terrorism, governments, with their ability to shape agendas across the complete spectrum of media, stand a much better chance of countering threats which do emerge from it.

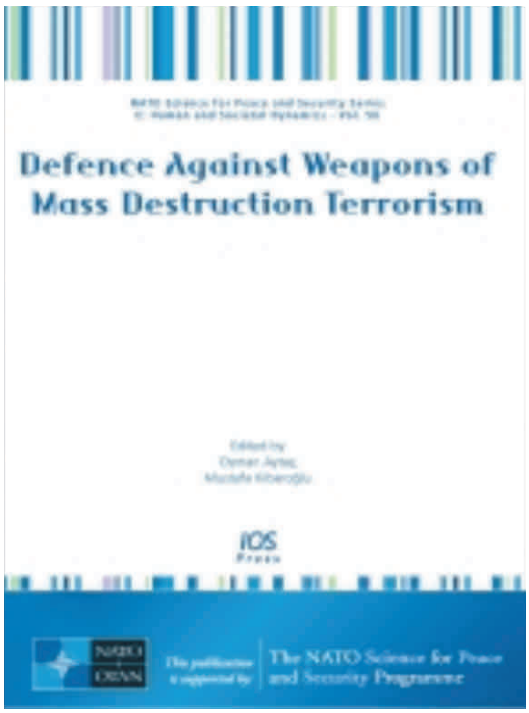
Divine religions or other types of communal spiritual beliefs and acts of terrorism can hardly have anything in common. Andreas Armborst provides a conceptual and descriptive clarification of the notion of killing in the name of a religion by presenting a variety of definitional features. The author argues that as part of the efforts of clerics and jurists over the centuries to adjust Islamic international law to social-political realities of their time in a sophisticated manner, today's reformists seek for a non-hostile interpretation of jihad.

Because terrorism has become truly global, the link between terrorism and how it changes the foreign policy framework of the states gains much currency. Itu'ddr Toksö'9az studies the concept of threat in international politics and deliberates on the types, as well as the old and new usages, of the term of instability. The author argues that without a good understanding of what is domestic and what is international concerning threat perceptions, the role of the military in foreign policy making in the post-Cold War era cannot be fully understood.

It is a well know fact that while states must be successful in their efforts to protect their citizens and their strategic assets at all times, terrorists need to be successful only once. Hence, intelligence and security services work hard to thwart any such attempts. Gordon Woo argues that terrorist targeting, attack mode and multiplicity can be analyzed, and the prioritization of targets for attack and defense can be assessed according to criteria of societal criticality, attack vulnerability, and terrorist capability. The author suggests measures to mitigate and avoid terrorism risk by adopting a risk-informed approach to counterterrorism resource allocation.

DATR always welcomes contributions from experts, civil and military officers as well as academics who have been involved, in one way or another, in defence against terrorism, which has become not just a professional undertaking of only a number of individuals in various capacities, but rather an overarching duty of all the noble members of the world's peace loving communities. There is no other way out, but to bring together the efforts of all the concerned body of intellectuals against the terrorism predicament, hopefully, sooner rather than later.

(Mustafa Kibaro¤lu, Editor-in-Chief, "Editor's Note", DATR, COE-DAT, Ankara, Spring 2009)



Defence Against Weapons of Mass Destruction Terrorism

Editors: O. AYTAÇ, M. KIBARO/LU
Centre of Excellence Defence Against Terrorism (COE-DAT)

Volume 56, NATO Science for Peace and Security Series
E: Human and Societal Dynamics

Publisher: IOS Press –Amsterdam
July 2009, 184 p.

In Defence Against Weapons of Mass Destruction Terrorism the editors examined the class of Weapons of Mass Destruction (WMD) for terrorist use and have found that their effects range from serious nuisance value up to catastrophic destruction of a large urban area. There are some differences in the effects depending on whether they are used against military or civilian targets, whether they are used from inside the target area or outside, and between those weapons for which MOPP (Mission Oriented Protective Posture) gear can provide useful protection (Biological Weapons, Chemical Weapons) and those for which it often cannot (radiation, nuclear explosions). These are useful ways to begin thinking about establishing protocols for protecting our armed forces and the civilian population they are sworn to defend.

This study is the result of the Defence Against Weapons of Mass Destruction (WMD) Terrorism Advanced Research Workshop funded by NATO's Security Through Science Programme held on 10–11 April 2008 in Ankara, Turkey under the guidance and the direction of the Centre of Excellence Defence Against Terrorism (COE–DAT).
The workshop aimed to provide a forum for exchanging information on WMD related issues, to enhance understanding of the nature of the threat posed by WMD terrorism and to discuss ways and means to counter the threat. This book project should be seen as an attempt to lay the basic groundwork for future research and study of the subject.
The editors would like to acknowledge the contributions of the co-director of the workshop, Col. Teimur Zavrashvili from the Georgian Ministry of Defense.
The merit this volume is ultimately due to the arguments and insights of the authors whose essays are collected here. We are grateful to them for their contributions to this volume.
(O. AYTAÇ, M. K‹BARO/LU, "Preface", Defence Against Weapons of Mass Destruction Terrorism, Amsterdam: IOS Press, July 2009.)

NOTES

NOTES