CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM

COE-DAT
# Newsletter
Volume 2 / Issue 7 / July 2008

## Content

3 **General Overview of the Terrorist Activities**
by Ergün ERÜN
Major, (TUR AF)

8 **Concept Reshape Warfighting and Transform Security**
by Mitko STOYKOV
Ph.D. Col.Eng. (BGR A)

18 **International Strategic Cooperation in Asymmetric Warfare and The Problem of Defining "Terrorist Organization"**
by Assoc.Prof. Çınar ÖZEN

22 **Terrorist Group Formation and Recruitment**
by M.Uğur ERSEN
LTC (TUR AF)

32 **Terrorism as a System**
by Erdoğan ÇELEBİ
Captain (TUR A)

38 **COE-DAT Activities**

COE-DAT;

Your gate to get information.

## Editorial

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

Col. Mitko STOYKOV, points out that the transformation of existing social structures and global problems like increasing of population, the global warming, the networked terrorism, the deeper energy and economy crisis, and limited world's resources, provoke the need of new applicable security policy. Within this framework, He seeks to identify how the information and the information technologies work positive and negative in society transformation and what their role for increasing effectiveness of the security systems are with respect to the concepts of Cyber War, Information War, Netwar, and Network Centric Warfare.

Assoc. Prof. Çınar ÖZEN, examines ideology and propaganda as the vital elements in asymmetric warfare in his article on *International Strategic Cooperation in Asymmetric Warfare and the Problem of Defining Terrorist Organization*. In this context, he emphasizes why and how terrorist organizations use asymmetric warfare, media's role as a propaganda tool, terrorism and insurgency as two different phenomena, and the international cooperation in the fight against terrorism.

In his article on terrorist *Group Formation and Recruitment*, LTC M. Uğur ERSEN tries to provide important aspects of recruitment process of terrorist organizations by putting forward why terrorist organisations need recruitment, how and when being a terrorist becomes attractive, characteristics of target population and recruits, recruitment methods and models, post-recruitment process and ways to counter recruitment.

Capt. Erdoğan ÇELEBİ argues that terrorist systems are open systems that have some unique characteristics. As indicated in his article on *Terrorism as a System*, terrorist systems tend to be self stabilizing, are or appear to be purposeful, capable of using feedback to modify their behavior, can modify their environments and capable of replicating, maintaining, repairing, and reorganizing themselves.

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

# General Overview of the Terrorist Activities (April - June 2008)

**Ergün ERÜN**
*Major (TUR AF)*
*COE-DAT*

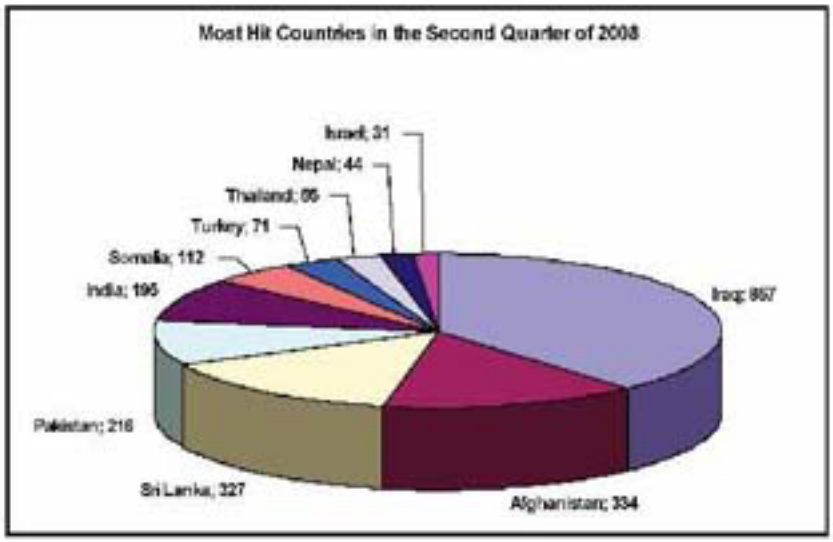
In the second quarter of the year 2008, some 2.396(1) terrorist incidents were recorded worldwide. These attacks claimed 4.204 lives and 7.614 injuries in sum. 319 people were also reportedly abducted by unknown assailants. Among the countries hit most during the year, Iraq was far and away the most hit one. The level of violence was almost same in the country when compared with the figures of the incidents in the first three months of the year 2008. In the period, some 857 separate attacks claimed 1.575 lives and 3.247 injuries more. That is to say that, 35 % of the total attacks in the world; 37% of the total fatalities and 42% of the total casualties sustained worldwide was recorded in Iraq.

The capital Baghdad was the epicenter of the violence with 291 separate terrorist incidents. These incidents claimed 575 lives and more than 1.200 injuries in the period. Also, an upsurge was also observed in the northern areas of Iraq. In Mosul and Kirkuk, totally 258 separate incidents, terrorist violence claimed 258 lives and 827 injuries. Additionally, 54 people abducted by unknown assailants in the northern part of the country.

Beginning with the spring in April 2008, the violence escalated in **Afghanistan** and terrorist incidents doubled when compared according to first three months of year 2008. Some 334 separate attacks in the country claimed 564 lives and 684 injuries in sum. The single deadliest attack in the country was reported from Kandahar on February 17 when a suicide bomber killed almost 26 people and wounded more than 12 others near a police station in Afghanistan's western province of Farah. The attack was noted to be the deadliest one in the second three months period in Afghanistan. The southern Kandahar and Helmand provinces were the most volatile places in the country both in terms of the number of attacks carried out and the level of casualties sustained. Indeed, 111 people lost their lives and 107 more sustained injuries in 41 separate attacks in Kandahar while some 33 attacks claimed 61 lives and 60 injuries in Helmand. In addition, the eastern capital city of Kabul, Ghazni, Paktia and Paktika province were also hit hard in the relevant time period and totally some 86 attacks killed 95 people and injured 170 more.

| | Country | Event Count | KIA | WIA | AIA |
|---|---|---|---|---|---|
| 1 | Iraq | 857 | 1575 | 3247 | 103 |
| 2 | Afghanistan | 334 | 564 | 684 | 17 |
| 3 | Sri Lanka | 327 | 386 | 1509 | 2 |
| 4 | Pakistan | 216 | 316 | 463 | 74 |
| 5 | India | 195 | 301 | 422 | 28 |
| 6 | Somalia | 112 | 661 | 466 | 8 |
| 7 | Turkey | 71 | 38 | 88 | 0 |
| 8 | Thailand | 55 | 43 | 135 | 0 |
| 9 | Nepal | 44 | 14 | 116 | 9 |
| 10 | Israel | 31 | 8 | 62 | 0 |

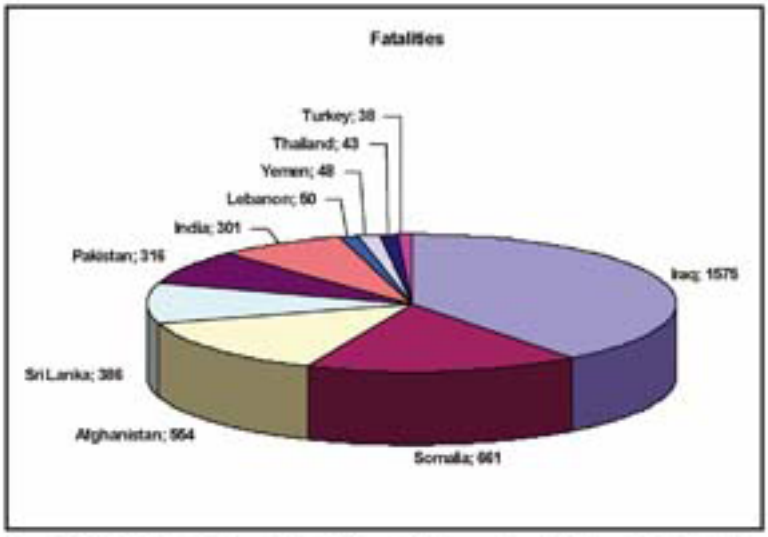
Table1 - **The Most Hit Countries Worldwide**




Graphic 1 - **Worldwide Most Hit Countries in the Second Quarter of 2008**

*(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.*

The intensified clashes between the security forces and the Liberation Tigers of Tamil Eelam (LTTE) terrorists in **Sri Lanka** made the country the third-most hit one in the world. The level of violence in the country has increased in the second three months period of year 2008. Consequently, 386 people, including the members of the security forces and the civilians, lost their lives and 1.509 more sustained injuries in separate 327 incidents. The amount of the terrorists neutralized in this period was much higher than the casualties sustained to the security forces. In general, the close quarter armed attacks, indirect fire attacks and landmine usage were the main tactics of the terrorists in the country. In addition, three suicide attacks, one of them against civilians in Weliweriya, were reported from Sri Lanka and claimed 36 lives and 188 injuries in sum. The suicide attack against civilians carried out in Weliweriya19 Km northeast of Colombo, **killing 14 civilians including the minister of highway and road development,** Jeyaraj Fernandopulle, the runners for flagging off the race. K.A. Karunarathna, the former national marathon champion and South Asian




Graphic 2 - **Ten Countries Those Gave the Highest Fatalities in the Second Quarter of 2008.**

marathon gold medalist, Luxman Alwis, the national athletic coach and Chief Inspector K.D.R Kannangara, personnel security officer to the minister were also among the dead. In the suicide attack, **83 people also wounded.**

In **Pakistan**, the violence continued in the second quarter of 2008 with some 216 separate incidents, killing 316 people and wounding 463 more. Although a little escalation was noted in the second three months period of the year 2008, the casualty levels didn't show a similar trend. The level of fatalities remained lesser than the first three months period. The deadliest attack in the country was reported from Kyber Agency. Fighting erupted between loyalists of militant group Lashkar-e-Islam (LI) and men of the Kooki Khel tribe of the Khyber Agency on April 16, following three days of tension. At least 20 people had been killed in the clashes. No suicide attacks reported in April 2008 in Pakistan, But in May and June 2008 six suicide attacks, the deadliest one happened in Mardan, claimed 34 lives and 76 injuries. In Mardan, a suicide bomber killed at least 13 people on May 18, in an attack close to the gates of an army training centre in the northwestern Pakistan. The bomber was on foot and blew himself up outside the gates and close to a bakery shop in the military cantonment area.

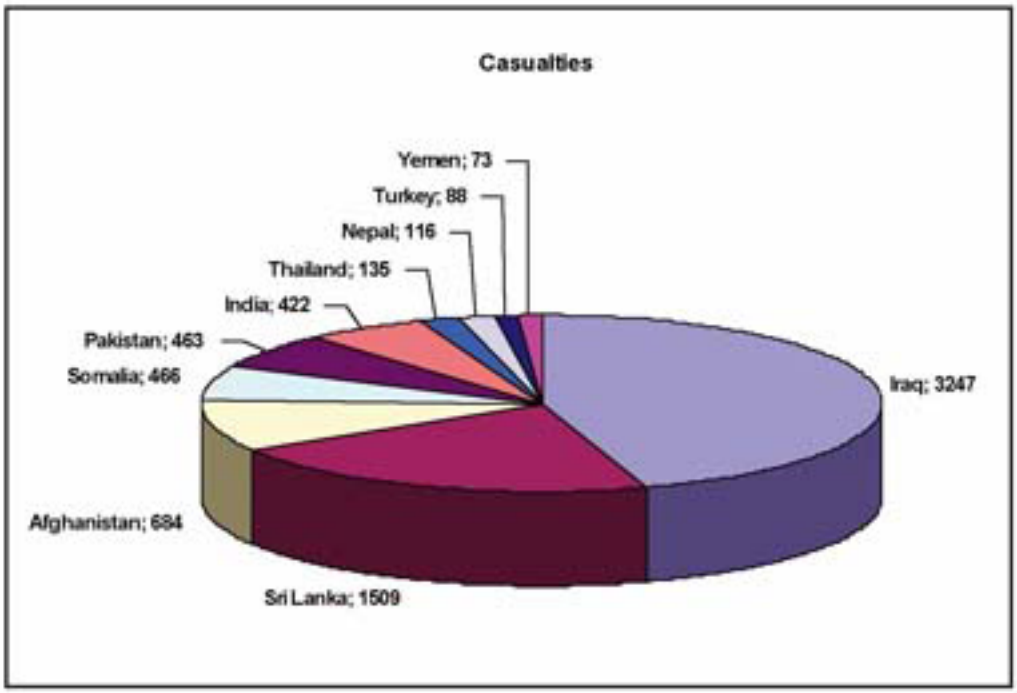
The level of terrorism related violence in **India** in the second quarter of 2008 was almost the same in the first three months period of 2008. In the second three months of 2008, 195 separate attacks, killing 301 people and wounding 422 more, put the country on the fifth place of the most-hit countries standing. The deadliest attack in the country was carried out on May 13 in Jaipur. At least 80 persons were killed and over 200 others wounded when eight serial bomb blasts were triggered at Johari Bazaar, Hanuman temple, Hawa Mahal, Badi Chaupad, Tripolia Bazaar and Chandpole in Jaipur, capital city of Rajasthan. The first blast took place at 7.20pm in the crowded Johari Bazaar and within 15 minutes seven more blasts occurred in adjoining areas in the walled city area, near the Hanuman Mandir, which was reportedly crowded with devotees, near Hawa Mahal, at Badi Chaupad, Tripolia Bazaar and Chandpole. Preliminary examination of the blast site indicated the possibility of ammonium nitrate being planted in new cycles and filled with ball bearings and small iron pipes to act as splinters.

Terrorism related violence in **Somalia** claimed 661 lives and 466 injuries in separate 112 attacks in the relevant time period, making Somalia the most hit African country. The improper information flow from the country, once again, hampered the efforts for a comprehensive assessment, but according to the information available, a monthly average of forty terrorist attacks was reported from the country. Undoubtedly, the most significant attack in the country was reported on June 18. In the incident, clash between religious-led insurgents and allied Somali-Ethiopian troops has killed at least 17 people.

71 separate terrorist incidents put the **Turkey** on the seventh place of the most-hit countries standing in the second quarter of 2008. These attacks claimed 38 lives and 88 injuries in the relevant time period. The main suspect of these terrorist incidents was PKK/KONGRA-GEL terrorists. The most volatile city in this period was Sirnak city. 17 separate terrorist incidents killed nine people and wounded 18 more in Sirnak city in the second quarter of 2008. But, the deadliest attack happened in Hakkari city on May 09. Turkish military sources said at least 20 PKK/KONGRA-GEL terrorists killed. Additionaly, **six Turkish soldiers lost their lives** and **two more soldiers wounded** after PKK/KONGRA-GEL terrorists attacked a military base in southeast Turkey.

The violence in **Thailand** continued in the second quarter of 2008 with 55 attacks, killing 43 people and wounding 135 more. Among the three troubled southern districts, Pattani was the most volatile one both in terms of the number of attacks carried out and casualties sustained with 20 attacks, killing 20 people and wounding 54 more. In addition, Narathiwat and Yala were hit for 30 times. The attacks in Narathiwat claimed 10 lives and 41 injuries while 13 people lost their lives and 40 others sustained injuries in Yala. The most significant attack in the country was reported from Narathiwat on May 05 when an IED was detonated in an iron box was planted in front of the house of the deputy provincial governor of Narathiwat and triggered by a digital watch Sunday night. Sixteen people including three girls were wounded in two separate bomb blasts among the latest separatist violence in insurgency-wracked southern Thailand.

The ninth of the most-hit countries standing in the second quarter of 2008 was Nepal. The intra-factional




Graphic 3 - **Ten Countries Those Gave the Highest Casualties in the Second Quarter of 2008**

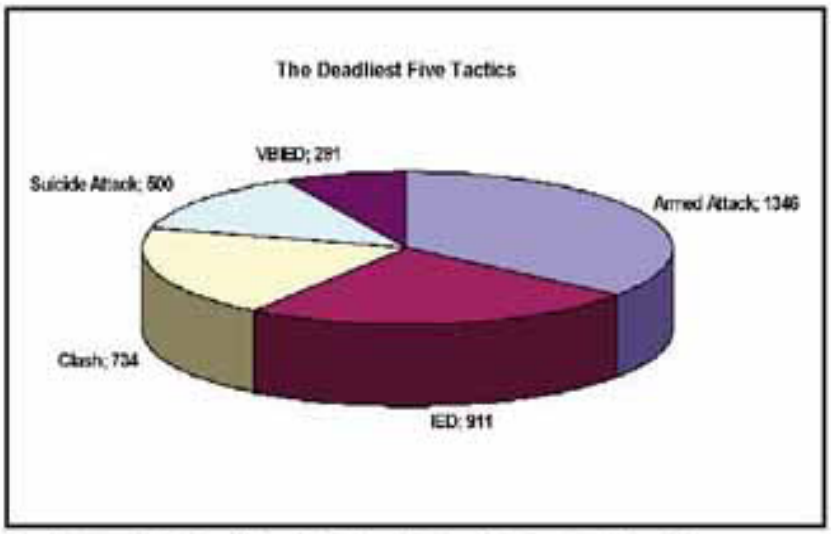
| | Event Type | Event Count | KIA | WIA | AIA |
|---|---|---|---|---|---|
| 1 | Armed Attack | 672 | 1346 | 575 | 9 |
| 2 | IED | 635 | 911 | 2418 | 2 |
| 3 | Clash | 344 | 734 | 1364 | 22 |
| 4 | IDF | 201 | 199 | 731 | 0 |
| 5 | Suicide Attack | 104 | 500 | 1258 | 0 |

**Table 2** - The Most Used Tactics in the World.

clashes and IED-attacks in **Nepal** continued in the relevant time period and some 44 attacks in the country claimed 14 lives and 116 injuries. The explosion in south Nepal's Rautahat district on April 09 claimed three people killed. The explosion occurred at Rajpur, Farhadawa, in Rautahat district, some 110 km south of Nepali capital Kathmandu. The blast occurred while the bomb was being assembled. Separately, in **Israel**, some 31 attacks claimed 08 lives and 62 injuries in the second quarter of the year. Undoubtedly, the violence in the country was marked by a rocket fired by Palestinian militants in the Gaza Strip injured more than 30 people at a shopping mall in the Israeli city of Ashkelon on May 14. The Popular Front for the Liberation of Palestine-General Command and the Salahudeen Brigades, a group aligned with Hamas, claimed responsibility for the attack, one of an almost daily pattern of militant attacks from the Palestinian enclave. Ashkelon, which is more than 10 km (six miles) north of the coastal enclave, has generally been out of range but some more powerful rockets, notably Soviet-designed Katyushas or Grads, have struck the city of some 120,000 this year.

The terrorists used fifteen different tactics in the second quarter of 2008. The traditional tactic of the terrorists, **the close quarter armed attack,** was the most used one with 672 separate occasions, targeting both civilians and security forces. At least 1.346 people were reportedly killed and 575 more sustained several injuries in these attacks. In addition, the **clashes** between the security forces and the militants caused considerable damages and 734 people, mainly the members of the security forces and the civilians in cross-fire, lost their lives and 1.364 people sustained injuries.

A wide usage of **IEDs** was also noted in the relevant time period and 911 people lost their lives and2.418 more sustained injuries in 635 attacks. Iraq was the most hit country by such tactic with 318 separate attacks. Afghanistan and Pakistan were also hit for approximately 200 times while more than 40 attacks were reported from Sri Lanka and India. Among the various IED-tactics, **suicide bombing** was noted to be the deadliest one as 500 people lost their lives and 1.258 more sustained injuries in separate 104 attacks. 54 of these attacks were reported from Iraq while Afghanistan was hit for 38 times. Pakistan was the other country hit hard with such attacks with six repetitions. The number of such attacks in Sri Lanka was noted as three while Algeria, Israel and Somalia were hit for once.




Graphic 4 - **The Deadliest Five Tactics Used in the World and the Fatalities Sustained.**

As another deadly IED-tactic, the **vehicle borne IED-strikes** also caused considerable damages in the world and such 71 attacks resulted in the deaths of 281 people and wounded 927 others. Iraq again headed the list of the most-hit countries with 60 occasions while Pakistan was hit for three times. Two such attacks were reported from Afghanistan and India while one each attack was carried out in Georgia, Israel, Spain and Thailand.

# Concepts Reshape Warfighting and Transform Security

**Mitko STOYKOV**
*Ph.D., Col.Eng. (BGR A)*
*Chief of Transformation,*
*COE-DAT*

The end of XX-th century broke the security framework of the "old world order" and unfortunately the beginning of the XXI-th didn't bring new one. Globalization and the boom of development of technologies boost level of insecurity and create the biggest challenges to our society on the way of achieving appropriate guaranties in building a new working security system.

The transformation of existing social structures and raised global problems – an unprecedented increasing of population, the global warning, the networked terrorism, the deeper energy and economy crisis, and limited world's resources, provoke need of new applicable security policy.

The information technologies influence's research on the changes in the global interconnected world and new means of a security policy bring together parts of several concepts: Cyber War, Information War, Netwar, and Network Centric Warfare. The main question here is: How the information and the information technologies work positive and negative in society transformation end what is their role for increasing effectiveness of the security systems?

The usage of well known different types of policy, system and structural analyses didn't bring the desired results in researching the new problems and the further lasted theirs unknown identity and influence show the limit of applied methodologies. Can new methods, based on contemporary social and economic theories, even still no entirely proved from the practice, bring better results?

The applying of the new structure-technological approaches of complexity theory's connectivity ant a research of the centric role of the information, could reveal changes in formation and function of the social structures, and help to find out their basis role for the security system transformation and the new means of generating power.

This approach could also allow simultaneously retracing and qualifying some mutually dependent processes running at the same time in the society – transformation, restructuring and mutation of social structures, increasing forms of achieving dominance over a new deformed manifestation of the security systems' threats. The importance of these problems calls for approved scientific, practical and historically valid principles, which are possible for development and future applying.

We can accept creating a purposefulness, timeliness and resources assisted defense policy as a significance evidence of made theoretical researches. Its importance for selecting proper doctrines, concepts, long and short-term plans will further increase in the future. Today existing approved effectiveness of new way defined military-political aspects of security and their role in interconnected collective security system also will rise. That's the way to try making forecasting together with existing practice and to apply results in security system transformation.

**An Analysis of the Choice and Management**

The limited opportunities of the many of so far applied methods of scientific analysis enable revealing only a minimal part of the specifics of the all arising problems in the current security systems. No entirely defined identity and incompletely shown effects of the impact of security system challenges continue to surprise not only the researchers, but also the managers of the security sectors. In the world of complexity and reduced predictability there is a great possibility the better result to be attained by applying newly designed, contemporary methods of research, based mainly on the new economic and social theories, with the understanding that so far a bigger part of them are still not completed and their practical applicability is still not entirely proved in all spheres of the knowledge and practice. With such a proviso this is an approach for application a new, different method of scientific research – an Analysis of Choice and Management – used for the research of the new information based concepts applicability.

A review of the basic characteristics of some concepts from the last decades - *Cyber War, Infowar(1), Netwar* and *Network Centric Warfare* could be very helpful to reveal the role of the common concept enablers – the information and the information technologies (ITs). The important impact of the concepts for changing the forms of warfighting insists on choosing a special methodology to study their practical application. The direct parallel between the role of these concepts for the determination of the future behavior of the entire security system and planned policies for the future of the other sectors of the society shows that a possible way for scientific research of the applicability of these concepts is the general idea of Michael C. Munger, introduced in his paper "Analyzing Policy:

Introduction to the Analysis of Choice and Management(2)".

The proposed method to analyze *Political Applicability* – searching for a good and applicable political choice, agreed methodology by means of selected criteria of effectiveness and equity, is an expression of a new, practically applicable approach to the studied problems. The usage of the equally acceptable criteria for all researches allows comparability of the attained results. A better authenticity of the evaluations is achieved by a commensurable sequence during the concepts' analyses. In order to assess the influence of the concepts over the changes of the forms of warfighting and transformation of security systems, to compare attained results, the following criteria are applied: technical applicability, value (cost), integrity with other security system concepts, and practical influence on the forms of warfighting.

**Cyber War**

The identity and basic characteristics of the concept Cyber War(3) are determined by a wider application of ITs – the contemporary base of the complicated electronic and cyber systems for management and control in almost all spheres of social life. ITs operate in a united Global Information Environment, which specifies the mutual dependence of all components in it. Along with positive influence of ITs, when the situation awareness of society for all simultaneously running processes is improved, there exists a clear tendency to increase the usage of these advantages for illegal and detrimental activities inside the same info-environment – contemporary available complex cyber systems are used irresponsibly from the criminal and terrorist radical groups in society.

What changes carries out concept of Cyber War?

It enriches traditional conceptualization by determination of new IT-based system - *cyber systems as complicated assistants or substitutes of people in operating, managing and controlling the complex industrial processes, infrastructure, financial institutions, defense and other spheres of social activity*. In the context of defense, the *Cyber War differs from traditional war with the capability to influence on security systems without acts of visible and direct violence*. It is directed to force the opponents to carry out the particular wills, which are attained by affecting the opponents' security (defense) systems with the utilization of software controlled processes. Broadly, among the warfighting activities of the concept of Cyber War can be outlined *cyber attack*, *cyber penetration*, *cyber manipulation* or *contortion*, *cyber hijacking* and *cyber disorganization*.

From the mentioned battle actions cyber violence influences and even changes the traditional forms of warfighting. Cyber penetration, cyber manipulation and cyber disorganization are no-sanctified, criminal actions -forms of cyber attack, and every cyber crime (as a action that no directly affects the national security) might be added to them. Depending on their dimension and influence over the national policy, cyber attacks might be considered as a form of Cyber War, because the final results (effects) over the national security may be compared only with those of a real war.

The increasing number, complexity and responsibilities of contemporary cyber systems expand the list of the potential target for cyber attacks. The need of effective operating armed forces management system transfers C4 ISTAR - (Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition and Reconnaissance) into one symbolic cyber target. Additional substantial targets for possible cyber attacks are all new warfighting platforms. The potential targets of cyber-terrorists are the infrastructure, management systems in economics, finances, health care, administration, security system and vital society services. Common cyber space is also an attractive challenge for continuously increasing activity of the terrorism. It offers an immense opportunity for costly adding of destructive symbols, even without visual tangible effects on society.

Except for new forms of offense, the concept of Cyber War offers also new ones of defense. The active methods of defense are materialized by using different software products – passwords to prove the user authenticity and special hardware coding counters, magnetic cards and preliminary coded hardware modules. The anthropomorphic methods utilize the unique features of a person - fingerprints, scanning pupils of eyes or person's face and etc. The multilayer defense tactics or the reiteration of the authentic confirmation of the admission rights is a defense method that uses answers to multitude inquiries of the system.

The application of passive methods of defense is a counteraction to the boom of the usage of technological or operational defects in electronic systems and social engineering – a principle means to affect the cyber systems. The priorities of access and the proof of connections authenticity

are the most applied methods for signal and physical cyber protection. The physical methods of defense include the isolation of the critical points of the information systems, establishment of critical management operations under manual control and the abolishment of individual control of software for the exceptionally important operations, reducing of the number of connections and level of integration among particular elements of cyber systems. The general methods of cyber counter-offense include all possible operations of identification - detection and reconnaissance, attack, destroy, pursue and capture.

The practical application of the Cyber War concept relates to the assurance of the protection of information infrastructure – one of the criterions, which really is a guarantee for the national security. A possible matrix of commitment and mutual dependence of all elements in an infrastructure could be exceptionally complicated. Thus, the most of the attempts to research this matrix are not very successful – in term of defining clear physical boundaries of the systems, as well of measurement of dependence and responsibility of the condition of each one element. With an increasing degree of the management dependence from computer software, the possibilities for cyber penetration grows up, and an increasingly presence of mega-management centers creates new single points of failure – the most attractive cyber-targets.

The development of an appropriate strategy, designed to defend the constantly changing configuration of the infrastructure forces the application of new methodology for access to the vulnerability of the infrastructure and for defining proper and clear priorities and criteria for success of it protection. Appropriate approaches to implement this strategy could include: a clear definition of problems, associated with the development and management of the infrastructure; conducting of adequate researches in the sectors of the infrastructure; general research of the management systems of the sectors and the whole infrastructure; outlining of particular measures and concrete technological and management solutions for the each of the revealed problems; development of appropriate measures to avoid the same or similar problems in the future.

The *technological applicability* of the concept is related to the saturation of the C4 ISTAR, defense platforms and civil sectors with new cyber systems - an exceptional opportunity to apply in practice all theoretical models for defense of the Cyber War concept.

The *value of implementation* of the concept is defined by a reasonable practical price for cybernization of our society. The value of military-political dividends from practical application of the concept in the modernization of the system and platforms, C4 ISTAR and improvement of the capabilities for defense of the vital elements from infrastructure is incomparable high, when compare with the price of all contemporary investments in ITs.

The cybernization of the military platforms and defense management systems is the best demonstration of impossibility to separate the concept Cyber War from the rest of concepts for operating armed forces in the security system. The *integrity of Cyber War with the other concepts* allows a realization of cyber-operations as an independent or as a permanent compound part of all types of the military operations.

The *practical influence of the concept on the changing forms of warfighting* is expressed by creation new diversity of the means and an huge potential - pledged in the application of different conceptual methods of cyber-influence; a comparatively low cost of the resources, which are needed for practical realization; a low level of risk, associated with implementation of the concept; an increase in the software managed systems – parameters that indicate an exceptionally high effectiveness from application of the concept and guarantee a new capability from practical implementation of the Cyber War. Therefore the concept of Cyber War directly influences and forces the changes in the forms of warfighting.

**Information War**

The advent of the concept Information War(4) renders a strong institutional, methodological and practical influence on the behavior of all social systems(5). Therefore it is accepted as one of the key elements of the new operational responsibilities of the security systems. Its application is directed not only to a better integration of all information in the command and control systems - C4 ISTAR, but also could be used as a base for conducting comparative analyses of

the conditions and capabilities, which affect the institutions of the opponents. Additionally Information War provides a methodology for a better organization and coordination of the security system's effort in providing optimal structures for operating of the information systems. It may respond to increasing requirements to the forces' structure, to need of building rapid reaction capabilities, to the implementation of the new technologies, to the increasing number of precise-aiming defense systems, mobile and deployment capabilities. Generally, the concept serves as an integrated strategy for better utilization of all available defense and security resources.

The concept Information War brought many new basic notions like *Global Information Environment, Military Information Environment, Defense Information Infrastructure.* The term Global Information Environment unites all persons, organizations and systems that have responsibilities to collect, process, disseminate information for different national and international consumers. Inside the Military Information Environment operate all military (and related) organizations of the security system of society. Defense Information Infrastructure is composed by all hardware elements of the networks of Defense Information Systems, which operate in the Military Information Environment. The increased connectivity of the information infrastructure broadens the list of potential threats for the security – from attempts of unapproved access to change and affect content of information in operating systems, to the substitution of all database, cyber attacks and collection of intelligence data, attempt to establish control on signals and overloading radiation, dissemination of false signals, conduct of psychological operations, overloading and falsifying content of free and independent media broadcastings.

The operational aspects of the concept - *Information Operations*, are conducted generally to influence the information and information systems of the opponents. At the same time their other main task is to create best possible conditions for protection own information and information systems. Both tasks are normally integrated in all phases of each information operation or mission - *intelligence, offensive, defensive, concomitant, political, economic* and other *information operations*. The *operational architecture*, purposely created for their conduct, allows building the necessary connections between the processes, functions, and organizations, involved in information operations. The *system architecture* collects connections between elements of C4 ISTAR and provides a physical connectivity inside the information systems. The *technical architecture* provides necessary system of regulations, which materializes and manages the connections between compound elements in building information systems and defining clear regulations for access to the system; connection; subordination; mutual dependence of the compound components and basic technical requirements; proper functioning and service.

The *technological applicability* of the Information War is determined by continuous development of the consumption and the market of IT-devices and services, which process, store and disseminate information. The establishment of Global Information Environment and Military Informational Environment is a real demonstration of the practical applicability of the concept. Despite the pervasion of ITs in the real world and the proved capabilities of the Information War, the lack of proper national concepts and system for planning and conducting information operations clearly shows a misunderstanding of the importance of the concept.

The *concept out* is associated with the causes for changing/enrichment traditional values of society. The decreasing identity of geographical boundaries, the capability to compress time, to wipe differences between personal and social property, to wear out the limitations between legal and criminal – all are the security system challenges, born by the new information environment. The information operations are peacetime alternatives for preserving the value system of society. Their effect - compared with sensibility of the defense resources consumption, increased effectiveness at the lowest possible cost – is a brilliant indicator for importance of the concept. Increasing the battle power with exploitation of the capabilities of Information War in the military operations and missions, and the possibility to affect public opinion, complicate the protection against Information operations and increase the meanings of the security systems and respectively the operational value of the concept.

The common usage of information in C4

ISTAR predetermines the *integrity of the Information War* in conceptualization the operability of the security system. It helps to increase effectiveness of all properties of exploitation information and ITs during execution of military missions and operations. It is an integrated strategy for better and qualitative consumption of resources, which is achieved by: adopting the possibility of communication in real time; increasing and sharing information; mastering shared situation awareness and information and decision-making superiority. The information superiority increases chances for success and new opportunities for real time planning minimize losses and their concomitant effects.

*The concept has direct practical influence on the changing forms of* existing forms *of warfighting.* The information operations are a basic or concomitant part of all the operations of the forces in peacetime, during the crises, conflicts and wartime. Their broad spectrum covers the political, legal, internal, external, criminal, geographical unlimited space. They integrate all available and potential offense and defense information-technological capabilities to help for the realization of standing objectives of armed forces or society. In time of increasing threats to national security, the information operations are conducted during the each phase of response of the security systems - as a part of preparation, training, deployment and rotation of forces, including all military and non-military operations.

The concept application on strategic level calls for a strict coordination between national, as well allied and coalition security institutions. The utilization of the concept in combined joint actions of a coalition is targeted toward the achievement of significant political, military, economic or information goals. Its main "target" is to affect the opponents' national level of considerable power and at the same time to protect your own forces and information systems.

On the operational level, the concept's goal is the realization of the large-scale important operational tasks - impact on the opponents' communication and information systems, logistic systems, command and control systems and protection of your own analogical systems and forces. The additional goals of the operations are breaking the opponents' capabilities to otganize, manage, deploy and support actions of their forces, and at the same time allowing an operational superiority of own forces.

The information operations on the tactical level are conducted to attain specific tactical tasks: influence on the adversaries' information and information systems, C4 ISTAR and it information based processes and provision of the best conditions for operating your own systems.

The Information War is an integral strategy, focused on increased states dependence and vulnerability from the information and information systems. For its practical realization it demands obligatory changes in the structure, management systems, technical equipment and tasks of the forces. It defines the modes of influence, targets acquisition and condition in a new way. Because of the highest effectiveness of the concept in all types of operations and the relatively low consumption of resources, the Information War is among the most applied concepts. The capability to generate warfighting power with exploitation properties of the increasing situational awareness changes the identity of the conducted missions, directly influences the opponent's appreciations and public opinion and additionally complicates the tasks of security systems. The characteristics, derived from the analysis of Information War, are a sufficient motive to concentrate more attention of the security systems on the concept. They outline an urgent and increasing need for creating information strategy and including it in the list of the urgent national security priorities.

**Netwar(6)**

The analysis of the presented from John Arquilla and David Ronfeldt *Netwar concept* (in their book "Network and Netwars: The Future of Terror, Crime, and Militancy(7)") embraces an increasing of network forms of organization in the society and their influence on its behavior, as well on the transformation of its security systems. The Netwar signals for the emergence of the new threats for society – different from the well-known wars. Their meaning is predetermined by the *influence of network structures on the forms of organization, doctrines, strategies and communication among the participants in the networks.* One brief examination of the influence of the concept on the newly posted: goals and intensity of conflicts,

threats for society, financial cost of consumption of resources and the results from their direct influence make it impossible to use different from war terminology.

Networks enforce the power of organizations because of the utilization of a better ability to conduct multi-channel communications, whereupon *the success of only one cell becomes success for the whole organization.* As designs of structural (operational) architecture, the networks unite all web-based and dispersed, but interconnected operational nodes (centers of activity). The nodes may represent persons, groups, formal and informal social organizations or even parts of them. As a dimension, networks might be small and big, purposely structured in tight networks or loosely grouped in opened or closed organizations, with common or narrow specialization. The boundaries of their structure might be determined with clear outlines or diluted in surroundings; the organizations look more flat than hierarchic; usually there is a lack of central or top leader, or even high-ranking commander; they are characterized by unprecedented broader local autonomy and initiative; the processes of decision-making and their implementation are highly decentralized and depend on a consensus, which is achieved thorough consultations. All these new conditions provide for the processes of decision-making, planning of operations and execution of missions to be totally free of the control and decentralized - dependent entirely from the achieved consultative and doctrinal consensus, which allows exclusively broad local initiative and autonomy of actions.

The structure of networks conventionally is divided in chain or linear network – hub or star, full-matrix or full-channel network, different types of hybrids of the cited models and possible mutations of every one of them. To the list of types of networks might be added so called *swarming strategy* – actions of special coordinated invariable or pulsated impact from all sides toward a particular target. The main offensive characteristics of networks are adaptability, flexibility, agility, and steadiness to challenges. The defense potential of the network organizations is built with utilization diversity and multi-layers, power and endurance. Because of the specific interoperability of the networks, the complexity of the elements and the lack of a necessity for central command and control, the organizations are difficult to decipher and destroy.

In the Netwar concept, the *terrorism is scrutinized as a weapon of the weaker, an asymmetric attack and defeat of a stronger opponent, also as an activity of groups on ethno-nationalistic, racial, religious-fundamentalist or minority basis.* It is considered as a tool of advertising, verifying and defending the personal and organizational identity, and by deliberately destroying the present, it might be used for attaining and approving a new "world order". Contemporary terrorism evolutes in the direction to Netwar and this process help for the internationalization and globalization of terrorist organizational structures. The effective counter-terrorist actions insist on new consciousness to the terrorist threats because terrorist organizations master new "holes" in the structures of the security systems. At the same time a new net-directed transformation of the security system and a multi-structural stuffing "holes" with an integrated interoperability on the legal base might provide for a better utilizing ITs advantages.

The *technological applicability* of the concept Netwar is a prediction of the future domination of net-based conflicts and network forms of warfighting, because the Information Revolution declares and manages not only the increasing network form of organizational structuring, but also reshapes the forms of the conflicts.

In time of revolutionary changes, the information and ITs have a winning value for development of network organizations and doctrines. The possibility for their success depends on a wider connectivity of organizations; applying capability to disperse/share information among the cells in the networks; the diversity of information and possibility to receive, store, process and disseminate information. The operating of multi-hub and multi-channel constructions insist on, depend on and force building a special infrastructure for communication, dense connections and functional information. The fast development of ITs and their relatively low cost favors building, upgrading and exploitation of the integrated network structures in the contemporary security systems as well as guarantees attaining superiority and final success.

*The value of the practical implementation* of Network is imposed by the broadening spectrum, intensity, geography and mutual dependency of "hot spots" in the world, a proof for domination of the Netwar conflicts in 21-th century. The importance of changes is committed to the challenges coming from the need for deep alterations in hierarchical apperceptions, behavior, structures, doctrines and concepts. The change of bedrock notions of society, driven by increased mutual dependency and globalization, will force the setting of network subjections in the heart of the transformation of society.

The *integrity with other concepts* in security systems shows that Netwar is an inseparable part from the conceptual chain that utilize the increased role of information and the new achievements of ITs. The concept integrates theory and practice of the anterior concepts Cyber War and Information War, and as a higher stage also might be a base for upgrading. The main value in this chain of conceptual development is defined by a successful attempt to explain changes in all spheres of social life, with a significant attention on determination of the new character of security threats and possible means to resolve problems, associated with them.

The next dominating model of the Netwar conflicts declares the practical influence of the concept on the form of warfighting in existing social system. Network forms of structural organization, doctrines, strategies and communications affect their identity. Netwar examines the possibility to generate battle potential in the internal structures of network organizations. Network power is considered a real consequence of obligatory permanent connectivity of internal cells. The existence of connections does not mean constant communication; it is only capability to communicate in need.

Applied for the first time unconsciously by the terrorism, the concept demonstrates a possibility of the weaker to conduct asymmetric attacks and to destroy stronger opponents, copulating actions on racist, minority, ethno-national, and religious-fundamental base. IT-evolution internationalizes and globalizes these organizational structures that utilize structure holes between state institutions in the security system of society. An effective counteraction to this process call for awareness of the real threat and timely network directed transformation of the structures of security systems.

**Network Centric Warfare**

The concept *Network Centric Warfare(8)* is a relatively new attempt to integrate and summarize tendencies of the increasing number of the information based methods and means of operating the security systems. ITs are DNA(9) of the Information Ages and serve as a base of many new concepts and practices, which allowed our society to feel more comfortable when is embedded into the net of the Global Information Environment.

The access to needed amount of qualitative information and its effective utilization is a excellent base for proper decision-making. Therefore the needs for steady access to an immense volume of information, for new devices to overcome of the limitations of time and space and to increase reactivity require new unprecedented speed of processing of the information. The skill to work in the saturated information environment serves as a base and catalyser of changes in the means of creating prosperity and military power. It is also accepted as a new way for creating a new type added value for society that is compatible with the results of the revolutions of previous centuries.

The inherent for the security systems need of unification of the geographically dispersed armed forces in specially designed provisional teams for execution of planned operations leads to increasing the number of organizations simultaneously operated in the integrated battle space. The term Network Centric Warfare is a new product of network centric thinking – a result from utilization the advantages of the network-structured organizations. It characterizes the new potential and power, which are generated from the increasing level of awareness in the management of geographically dispersed forces and applied in Network Centric Operations. The elimination of geographical-location and time limitations guarantees a success of the next step that follows the change of the massing of forces and battle equipment into the massing of effect, helps to reducing risk, to eliminate cost limitations of conducted missions.

Network Centric Warfare introduces numbers of new terms. The information superiority defines a condition of desired imbalance or advantage in the information sphere; the practical and virtual awareness – the possibility to possess needed quality and quantity information in proper form, and time; and reciprocally – to impede the opponents for reaching the same state.

The connectivity of structures allows an access to network centric segments of the information sphere of the battle space (space of missions, environment), where the notions of operational situation and joint planning of missions are concentrated. Their existence is proved by centricity of information, achieved by means of contemporary communication devices.

The information network is the infrastructure of network centric computerization – connecting, providing database, processing of information, automatic management of compound systems and communication among them. It provides all needed processes - receiving, storage, processing, transmitting and protecting of information, and operability of the system implants the information availability (achieved information superiority) in the processes of decision-making (as a decision-making superiority) and executing of tasks.

The operational architecture of the network of users allows enveloping timely and precisely planning and of the operations. Sensors' network consists of physical and virtual elements of the battle space, which provide for a constant, high level of situational awareness. The operations are planned and conducted in the network of users.

Dynamic shipment of sensors characterizes the process of providing an operational flexibility and reactivity, achieved by synchronizing situation awareness in the battle space to support tempo of operations. The synthesis of data in C4 ISTAR defines a possibility for sensor network to unite multi-spectrally information in the battle space for generating a higher level of situation awareness.

The forecasting initiated planning examines the possibility for advanced planning, conducted to avoid the direct confrontation in the battle space. It expresses a possibility to increase advanced readiness to exploit the full potential of capabilities of own security system. By applying joint command to forces, a dynamic synchronization of the components of forces and resources of missions is achieved in the battle space.

The *physical domain* of network centricity characterizes the sphere of direct reciprocal influence of forces in the battle space. The *information domain* represents the sphere of creating, processing and sharing of information. In the *cognitive domain* are situated apperceptions, awareness, understanding, believing, and values. They help in decision-making process, planning and execution of missions. The cognitive domain is an environment for personal qualities, morale, unity, training, battle experience, and public opinion. In this sphere is formed treatment to doctrine, tactics and Standing Operational Procedures. The *social domain* contains the network of relations among people and units. The assessment of the particular characteristics of all spheres is a summary of synchronization effect of the effort of forces in the battle space.

Several indicators determine criteria for network centricity. The *level of connectivity* of a particular force in the battle space does not automatically provide a network centricity to its actions. Achieving network centricity depends still on the *type and saturation of information, technological means of its exchange*, and the *capability of users* to acquire those qualities, which the cited characteristics give. The technical compatibility may be achieved on the different levels of connectivity of forces. Its exploitation in the real time can provide needed operational compatibility that directs influences on achieving every type of domination in the battle space.

The semantic compatibility creates a shared understanding in cognitive domain of the meanings of all processes that run in the battle space. It reflexes a capability for routine exchange of information among geographically separated in the battle space forces to create equal level of awareness and understanding of situation. The integrity of commanding is an expression of the maturity of network centric thinking, which is affected by capability for a real time, combined joint planning and command. The capability for joint command is a premise for integration of defense in the battle space. Except for the availability of network connected forces, network centric readiness insists on carrying out all liable conditions in the effort of information and command superiority to create a new value – increase of battle power and full battle space domination.

The utilization of the potential of *practical application* of the concept is an incident with the increasing capabilities to achieve common understanding of the "National security" term in the Information Ages, to work in the coalition environment, to achieve interoperability, to build and manage mission capability packages, to develop and apply a proper strategy for implementation of the concept, and to create needed educated and trained personnel. The practice of Network Centric Warfare can exploit the possibility rules, limitations, resources and goals of the missions to be united and managed in the network centric built mission capability packages (MCP). The MCP assembles in one portfolio Concepts of Operations, Combined Joint Command and Control, the force organization – structure, properties, and force readiness.

The possibility to estimate the capabilities of the each soldier, as well as of the whole security system, to conduct successfully a particular mission, goes through criteria of quality, derived from different spheres of the operating

of information (presented four domains – physical, information, cognitive and social). The final assessment depends on complicated interconnections between quality of information, the degree of information sharing, the influence of awareness sharing on increasing battle space knowledge, the knowledge sharing to attain a new knowledge state – knowledge superiority. This domination furthers to convert knowledge superiority in the decision-making and planning superiority – it generates real battle superiority on the base of new collaboration and coalition in the battle space, by the synchronization effect of the activities and transformation of the positive results from all running processes in the new battle capabilities.

Capability based planning is determined as a planning under deeper uncertainty, which provides possibility to answer to a broad spectrum of challenges and contingencies in the economy determined framework. The network centric executed capability based planning might be a possibility for new integral defense planning, a preceded desired portfolio management stage with a sober estimation of admissible compromises during phases of building capabilities of structure of forces; to serve as a force generation process; to help improve quality and quantity of platforms, to create the expeditionary capabilities and power projection, to conduct Effect Based Operations; to support employment of alliances, conduct of researches and inculcation of results on defense needs, including in period of transformation of forces-prototypes. A contemporary defense portfolio of the security system has to contain the expenses that are used to create present and close future capabilities of force readiness, the funds for change the battle space (communications, networks, and infrastructure), and the expenses needed to neutralize the influence of the security system over the environment.

The *technological applicability* of the concept is based on concepts and practices that allow of the society to feel more comfortable and more secure in the Global Information Environment. The synchronization of the situation awareness and dynamic shipping of the sensors provides operational robustness and flexibility, increased reactivity of forces and tempo of operations, and the users' network – the universality, timeliness and preciseness of operational planning, as well as realization these operational plans.

The *value of the concept* is determined by transfer of the skills to work in the saturated information environment and to catalyze new added value - military power, derived from the business management practice and applicable in the security systems. The meaning of value will increase with the grow of need for combining geographical dispersed organizations (forces) in special structures for executing particular tasks, and with increasing number of existed virtual organizations. The elimination of geographical-location limitations guarantees massing of effect, decreasing of the risk associated with operational uncertainty, reducing time-space limitations.

The result from concept application is creating additional desired added value –information superiority (command superiority) from exploitation of imbalance in the information domain of network centricity. Utilization of the practical or virtual awareness expresses a possibility to possess needed quality and quantity information in the proper form and time – proving centricity of information in created networks, and impedes the opponents (the enemies) to achieve the same state.

The *integrity with other concepts* is predetermined by summarizing and integrating the tendencies of increasing the relative portion of IT-based means and equipment for contemporary warfighting in the Network Centric Warfare. The concept characterizes the potential that is generated from the achieved level of awareness inside the geographical dispersed forces. This potential is exploited by conducting network centric operations, designed to fulfill the commander intent. Therefore the concept is a base for integration of all existing and future concepts in the security system.

The *practical influence of the concept on the form of warfighting* is defined by the conscious directing of the Network Centric Warfare concept to the changes of the entire spectrum of operations in the security systems. In the C4 ISTAR system, the access to the needed quantity qualified information and its effective profit are the best base for making the correct decisions, and the need for a permanent access to huge amount of information, for overcoming time and space limitations, from an increased reactivity force a constant increasing of speed of the information processing. The combined jointness of the information or the synthesis of data in the C4 ISTAR characterizes a capability of the sensor network to unite multi-spectrally information in the battle space for generating a higher level of situation awareness. The possibility for the forecasting initiated planning is aimed to avoid the direct confrontation in the battle space and to increase preliminary readiness for utilizing the whole potential of the own forces. By implementation of the combined joint command and control on the forces, the concept is a new opportunity for dynamic synchronization of geographically dispersed components of forces and resources of the missions.

During the change of the form of the influence on the opponents, by conducting

Effect Based Operations and existing real possibility for creating a cascade of effects, by application of control on summarized assessment of the effect of synchronization the effort of all forces in the battle space, by providing fast and precise identification and access to the targets, their prioritization and acquisition, the concept guarantees the success when implemented in the missions.

Acquisition of the potential of practical implementation of the concept is related to the increasing opportunities for achieving shared understanding of the term "national security" in the Information Ages, working in the coalition environment, achieving interoperability, creating mission capability packages, developing and implementing a proper strategy for implementation of the concept, establishing the needed educated and trained personnel.

The applied method of analysis of the IT-based concepts gives one more new opportunity to find out connections between the motives for their creation and their possible influence on the transformation of security systems' structure and behavior. Common framework of the problem is the exploitation of the information paradigm's influence over the security system transformation. The effectiveness of the change management depends upon the proper answers of the questions for the usage of information and ITs for generating of new power, for their influence on the changes of the structure, management, collaboration and interoperability inside the security system. The used identical criteria for the assessment are applicable to research every security system concept, and the time of concepts' creation demonstrates the sequence of the theoretical and practical upgrading and mutual addition.

At the middle of the Information Ages the development of technologies leaves behind the adaptation of the society management and security systems to the increasing number and diversity of security threats. Therefore the overtaking changes affect the conceptual basis, organizational structuring, readiness and management of the security systems. New conceptualization of the means of warfighting and operating security systems will continuously reshape the organization of traditional warfare and provide new tools for change management or transformation of the security systems.

## References

*(1) Infowar – Information warfare;*
*(2) Michael C. Munger, Analyzing Policy: Introduction to the Analysis of Choice and Management, 2001, Duke University;*
*(3) James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, 2002, CSIS;*
*(4) G S Spiroly, Strategic Information Warfare, 2000, http://www.sm.ethz.ch/gipri/eng/STW.htm;*
*(5) Social System – globally a system with participation of people;*
*(6) Netwar – Network Warfare;*
*(7) John Arquilla, David Ronfeldt, What Next for Network and Netwars, 1999, RAND;*
*(8) David S Alberts, John J Garstka, Frederic P Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2000, 2nd edition, Library of Congress Cataloging-in-Publication Data;*
*(9) DNA - Deoxyribonucleic acid;*

# International Strategic Cooperation in Asymmetric Warfare and The Problem of Defining "Terrorist Organization"

**Çınar ÖZEN**
*Assoc.Prof.*
*Academic Advisor*
*COE-DAT*

Asymmetric warfare is a subversive method conducted against the state. In asymmetric war, special war methods controlled by a weak party acting against the state for various reasons are questioned(1). Vital elements in asymmetric warfare are ideology and propaganda. The main purpose is to create public mobility and to reach political goals by making the state unstable. Asymmetric war generally begins at the level of terrorist organization and aims to become insurgency.

Asymmetric war is both started and carried on by the terrorist organization through using specific methods.. Although it is called as "warfare", asymmetric war does not resemble classic warfare. The supporters of asymmetric warfare are not equal in terms of power, situation and opportunities. Appearance of asymmetric warfare also stems from this asymmetric situation. Asymmetric warfare is a concept which emerges from and puts forward the inequality of its parties. On the one hand this inequality which results from the limited capabilities of the terrorist organization, performing an armed propaganda, in comparison with the state indicates a conventional power imbalance. On the other hand, this also expresses the feature of the terrorist organization, creating huge political effects with limited tools .while standing on the weak part of this asymmetry

Terrorist organizations do not have the power to defeat the state militarily. Knowing this very well, they use asymmetric methods in their struggle. As a result, asymmetric warfare stands as a "war of attrition" and presents prolonged, tiring and source consuming characteristics. Terrorist organizations in asymmetric warfare do not aim to win through conventional tools at the tactical level. The purpose is to set out political targets in their strategic plans and force governments to accept these targets by intimidating them. Accordingly, these organizations use violence as a propaganda tool and not for a military victory.

Armed propaganda aims at both the state and the public. Terrorist organizations executing an asymmetric struggle evaluate the targeted mass in two categories; potential sympathizers and enemies. Organizations perform two different tactics for each group. Terrorist organizations classify the government and the public, perceived as enemies, in the same category and aim to create fear by using similar tactics for both. Because of this, terrorist organizations choose innocent civilians as targets in their activities in to create fear among people and make the government stand back. On the other hand, terrorist organizations try to force and encourage people that are considered as potential supporters to act according to its political purposes. Therefore, while they try to influence their potential sympathizers terrorist organization targets in their violent activities specific and selected groups and people. While terrorist organizations direct their violent activities towards state officials so as to encourage its sympathizers, they also perform activities to punish those who do not collaborate in order to force potential supporters to make a preference. By this method, terrorist organizations try to show the state in weakness and at the same time they want to put pressure on their potential sympathizers. This strategic fact clearly demonstrates that restricting the definition of terrorism only with j violent activities against civilians is not correct.

In asymmetric war, media is an important tool, even a weapon. Abrahms emphasized the vital importance of the relation between media and the terrorist organizations because these organizations cannot posses sovereignty over communication channels owned by the state. According to Abrahms, terrorist organizations can maintain the necessary oxygen for their existence as long as this relation is established(2).

Terrorist organizations try to use the media's power very effectively to influence the public. However, the state also has its own media strategy against them. Therefore, the use of media is shaped on the basis of the political will of asymmetric warfare parties. On one hand, asymmetric warfare goes on at the media platform. However, another important side here are the third states and the third party media. Third states and/or political groups within them take sides in this struggle through their own media tools. The most typical indicator of this appears over the definition of terrorism and terrorist organization. Using the principles of objectivity and impartiality as a pretext, third party media sometimes does deliberately define the party that performs

subversive methods in an asymmetric war not as a terrorist organization but as insurgents, rebels or freedom fighters and thus it supports indirectly the terrorist organization in this struggle. Third parties are included in the asymmetric warfare through the definitions of their own media. It is not necessary to be directly part of violence to take sides in asymmetric warfare. In asymmetric warfare, propaganda is the main tool instead of violence. Therefore, being the part of propaganda means being part of asymmetric warfare.

As it can be clearly seen in the example of Turkey, avoiding naming the PKK as a terrorist organization and instead using the term of rebel is the the most evident practice. Actually, defining terrorist organizations that are involved in asymmetric war as rebels is an example of the efforts for legitimizing them in the international platform. Consequently, third party media's definition of terrorist organizations as rebels, guerillas or warriors puts forward its will to stand by them in a political position and interfere in the struggle indirectly.

This kind of attitude, which finds place clearly in media companies like BBC, Associated Press, Washington Post, is evaluated by Turkey as unjust(3). The so-called impartiality and objectivity claims of BBC are not certainly valid for Turkey in the light of these remarks. It is also important to clarify the relation between governments and media foundations. The efforts of these media foundations to show terrorist organization as rebel or guerilla groups, attributing to so-called spokesmen of terrorist organizations in news, presenting terrorists as innocent, compassionate, brave people in photos, showing Turkey and this terrorist organization as equal sides in their style calls attention to the importance of this subject. The PKK is a terrorist organization, aiming the Turkish nation to accept their separatist call through armed propaganda . This insistence stems from their effort to provoke an insurgency in the South-East Anatolia region of Turkey at which they have been unsuccessful. It is not difficult to perceive or recognize the roles and political purposes of various third nations that are in search of self-interest especially in the Middle East geopolitics equilibriums. In the light of these evaluations, it will be beneficial to think about the definition of terrorism and insurgency once more.

Rosenau suggests that although terrorism and insurgency have similarities, these are indeed two different facts(4). At strategic level both of them are subversive activities of groups that are armed, in the form of non-state actors in their efforts, using violence to make their political programme accepted. Terrorism is about relatively rare activities of a militarily weak group targeting civilians to influence public opinion. On the other hand, in insurgency there are militarily more active groups having geographic control. While terrorism is considered to be the tactic in the early period of a weak activity, it aims to become militarily powerful and to gain the ability of practicing insurgency tactics.

In practice, the same organization applies terrorism and insurgency tactics relevant with the conditions and its power aiming to find and increase supporters for their political programme. The terrorist organization aims to affect both the public and the government by using violent methods within its political agenda. In addition to terrorist attacks, the terrorist organizations may apply insurgency tactics, and vice versa, as long as it maintains area control. In other words, terrorism and insurgency tactics stand as two sides of the subversive activity that appear in the form of asymmetric warfare targeting the state. These two type asymmetric warfare are identical at the strategic level but they differ at the tactical dimension based on the conditions.

The debate regarding the concepts of terrorism and insurgency has increased after the attacks of 9/11. Following 9/11 attacks, asymmetric methods have ceased to be an threat at the state level and spilled beyond the national boundaries. Many terrorist organizations appear to be active in global scale under the influence of "Political Islamism", and start to behave in coordination. These organizations act as connected and coordinated at the global level with the help of technological opportunities. In theory, these organizations aims political power at the national as well as global levels. These new terrorist organizations, which resemble the features of terrorist organizations in the asymmetric warfare literature based on class-rooted global struggle, have created a new and serious threat in the international system. The vacuum occurred following the end of

the Cold War and the loss of power of class-based ideologies have been filled with Political Islamist ideology. However, the main characteristic of this new asymmetric is that there is not any clear powerful state sponsorship behind these terrorist organizations. Although new global asymmetric warfare is executed at the global level, it carries similarities with asymmetric warfare methods conducted at the national level. In other words, these new terrorist organizations that perform activities at the global level act with national asymmetric warfare tactics.

The fight against these global terrorist organizations should be organized at the global scale. At the same time it necessitates similar tactics used by the state at the national level. This can be possible through the foundation of a powerful international coalition that will undertake the state's national level role. An international legal framework has to be formed in this regard. This is the reason of the intensified efforts for establishing a new international counter terrorism regime following the 9/11 attacks. These studies inevitably gave way to the discussion concerning the definition of "international terrorism" and at this point the reality that political will of states can change relating to their political choices appeared again. The understanding of "coalition" necessitates a consensus regarding the identification of terrorist organizations and definition of terrorism in general.

While creating a the counter terrorism regime within the international law, the concept of "terrorism" has been defined conceptually and "insurgency" has been taken out of this context. Accordingly, the terrorist organizations with which the coalition will struggle are identified as terrorist organizations and the ones out of the struggle are defined as insurgents, guerillas, warriors or freedom fighters. In other words, organizations that take place in the insurgent category are evaluated as legitimate at the combatant status and international regime has been recommended that is established by Law of Armed Conflicts for the struggle against them. On the other hand, there is no legal right in international law for organizations described as terrorist organizations. These organizations that commit crime against humanity have been defined legally as "illegal combatants".

The Geneva Convention gives legitimate and legal status under the title of "combatant" to the non-state groups that are supposed to have certain conditions. Rights and obligations are given to these groups in terms of international law. Some terrorist organizations have been in an effort to become legitimate subject of the Law of Armed Conflicts in case of fitting this definition without having state quality. It can be beneficial to point out that these conditions have a big uncertainty and political purpose becomes clear in the defining process. Consequently, the purpose of some states' evaluation of some of these organizations that perform asymmetric violence activities under the title of insurgency rather than terrorism stems from their effort to include them in legitimate combatant status.

In this legal argument, efforts to improve the concept of "illegal combatant" have a special importance. "Illegal combatant" has been put forward as a concept that will fill the gap in international law in the defence against terrorism. USA and Israel define some terrorist organizations that use insurgent tactics intensely as "illegal" under the justification of not fitting the conditions of Geneva Convention. Moreover, they prevent efforts of these groups to benefit from Law of Armed Conflicts and at the same time they can benefit from the opportunities of Law of Armed Conflicts as unilateral in their defence against these organizations. In other words; while the term of "illegal combatant" enables the states to use special practices of war legally against terrorist organizations, it does not provide any right that result from Law of Armed Conflicts to terrorist organizations.

Overall, definitions of terrorism and insurgency have become crucial for the states which deal with asymmetric war in terms of legal consequences. Turkey is facing the destructive activities of the PKK terrorist organization for more than 30 years. This dark war forced Turkey to be much more careful about these issues. In this context, it also became compulsory for Turkey to follow the international regime in the field of international terrorism closely. Because of this, Turkey is closely related to the arguments about the concepts of terrorism, insurgency and the international regime that developed in this context. Furthermore, Turkey is

interested because some western nations, with which Turkey takes place in defence against terrorism coalition, insistently do not identify PKK as a terrorist organization but evaluate it under the title of insurgency. Although international organizations and states added the PKK as a terrorist organization to their lists, this time Turkey faces tough attitudes of non–state actors and especially big media groups. These western groups follow a policy that supports the PKK and its separatist ideology by using insurgency and rebel concepts. Therefore, Turkey's handling of its foreign policy and its attitude towards the global war on terror are affected from the very beginning from the conceptual argument over terrorism and insurgency and its reflections on the PKK and its reflections on Turkey.

Actually, this difficulty as a result of defining terrorism either at the political or legal level and distinguishing it from insurgency is related to the problem of states' political intentions that interfere in this argument. In order to make political intention clear, defining terrorist organizations is more important than terrorism. Even lists of terrorist organizations have significant functions in this context. The publishing of these lists by states and international organizations is an expression of this reality. Therefore, these lists form an important step for the solution of the problem. However, Turkey is face to face with the fact of treating organizations that are added to these lists as if they are not terrorist organizations. In other words, there is the problem of differential treatment of these listed organizations when it comes to practice. This diversity in practice is a different but crucial point to be stressed for the success of defence against terrorism in the international platform. When it is considered that the most important condition for the success of international coalition in the defence against terrorism is trust, it is more important to do necessary things rather than forming lists of terrorist organizations. Otherwise, my terrorist organization, your terrorist organization diversity will eliminate the trust and inevitably the spirit of coalition. That distrust environment among coalition partners will create a suitable platform for the success of terrorist organizations that have the tendency to use states against each other. Because of this, building trust in practice is a very critical point for the international success of defence against terrorism as well as defining terrorist organizations.

**References**

*(1) Lawrence Friedman, "Terrorism as a Strategy", Government Opposition, Vol:42, No:3, p.321*
*(2) Max Abrahms, "Al Qaeda's Miscommunication War : The Terrorism Paradox", Terrorism and Political Violence, Vol : 17, 2005, p.538.*
*(3) Sedat Laçiner underlines that the news published by BBC titled "Sympathy for Rebels in Northern Iraq" and in Washington Post titled "Kurdish Society of Soldiers" are good examples to be incorporated in text books regarding how a terrorist organization can be indirectly supported via media. Sedat Laçiner, "BBC, Washington Post ve PKK", www.stratejikgundem.com, May 13, 2008.*
*(4) William Rosenau, "Subversion and Insurgency", Occasional Paper : Rand Counterinsurgency Study, Paper2, 2007, Rand National Defense Research Institute, p.2.*

# Terrorist Group Formation and Recruitment

**M. Uğur ERSEN**
*LTC (TUR AF)*
*Course Director*
*COE-DAT*

**Introduction**

The aim of this paper is to provide important aspects of recruitment process of terrorist organisations. Under this topic, why terrorist organisations need recruitment, how and when being a terrorist becomes attractive, characteristics of target population and recruits, recruitment methods and models, post-recruitment process and ways to counter recruitment.

Before starting, it is useful to mention about some of the global problems that might be affecting terrorist recruitment. An important factor that should be carefully focused on is the effect of globalization on the economy. Today, the total wealth of the 500 billionaries in the world equals the total wealth of the half of the population while nearly 1.1 billion people are living on the edge of starvation and even below according to the figures of the World Bank(1). The gap among the developed and underdeveloped countires are increasing every year.

Another important factor we need to pay attention is the imbalanced population growth in the world. The population of the world is growing fast, but resources are limited and decreasing day by day. According to the UN estimates(2), the world population will grow 1.1 billion in the next 10-15 years and another 2 billion by 2050 (Estimate:9.2 B) and almost all of this growth will be in under-developed and developing countries, particularly in Asia, Middle East and Africa. At this point, some questions arise: Will these children get sufficient nutrition, education and social support? Will they be physically fit and psychologically healthy? How will the community succeed to keep them far from terrorism? Will they be prone to terrorism? There is a requirement to find satisfactory answers to these questions.

Additionally, these regions are disadvantaged in demographic and economic respects. High fertility yield a population pyramid with many young and few elderly, resulting in high young dependency ratios. These in turn put adverse pressure on education systems and produce large numbers of unemployed youth with dim economic futures and high potential for dissatisfaction. These conditions cause the young generation to be vulnerable to the terrorist organisations.

Although poverty, population growth rate and other similar problems are not the main cause of terrorism, they provide fertile ground for terrorism and are easily exploited by terrorist organisations that utilize terrorism as a means of employment. They also partly explain why terrorism has condensed in Middle East, Asia and Africa lately (For a better picture, we should also consider energy policies, global warming, breakdown of secular ideologies, promotion of cultural differences and so on). The chart(3) given below (Figure 1) reflects the figures of the most hit countries in 2007.

**2. Why Do Terrorist Organizations Need Recruitment?**

Terrorist organisations need to recruit new members in order to survive and continue their actions. They have several reasons for recruiting new individuals. First, they aim to be effective over a large area to reach their both declared and hidden goals.

Second, they play a dangerous game. They lose their members continuously with deaths and injuries in their attacks, arrests by security forces, escapes, their own punishment and power struggles inside the organisation and several other reasons. Therefore, a terrorist organisation cannot survive and fill the slots without maintaining continuous

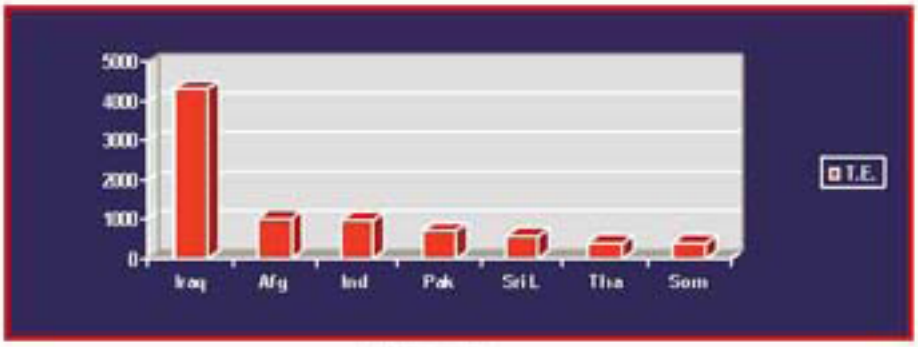



**Figure 1**

recruitment. As there are continuous missing in terrorist numbers, they have continuous recruitment efforts to compansate and continue their actions. Let's imagine that a factory loses many workers continuously. Can they survive or compete with others?
Another reason is the policy of the organisation to have limited experienced member. Because most members realize what the terrorist organisation actually aims after becoming a real member and that the ideals imposed during recruitment process do not match the current course of action, they gradually start to lose their motivation and rationale to stay inside and question their membership. What do they realize? They realize the ideals and goals told are not correct. They claim that they are fighting to protect the religion, but what they are doing is strictly refused in holy books. They claim that they are struggling for freedom and national values, but they kill innocent people from their own etnicity. We can find a lot of similar examples. This is what the leadership of the organisation is afraid of because it may cause a chain reaction and a quick dissolving.

The terrorist organisations try to avoid this motivation decline by discarding such members and recruiting fresh ones who are not aware of what is going on while keeping the most dedicated and experienced ones inside. They will find good reasons and methods to get rid of these individuals. The remaining terrorists who are loyal to the case will of course be in leadership positions and more professional. The circulation in the organisation and continuous recruitment prevents reasoning about the policy and actions and provides flexibility to change direction through different illegal actions.

### 3. How Does Being A Terrorist Become Attractive?

Now, let's discuss how being a terrorist become attractive. Human being tend to stray from legal basis and community values as they have too little to lose in their life. Looking at the Maslow's hierarchy of needs theory(4), as the individuals succeed to climb through higher levels, they adhere to the values more and they stay away from illegal actions in most cases. On the other hand, the individuals at lower levels are usually poor, unemployed, desperate and full of dissatisfaction. Lack of proper education, weak and ill family relations, problematic social relations and absence of moral values weakens the ties with the community and alienate the individual.

The individuals under these conditions are naturally prone to the illegal activities and motivations that are considered negative by the majority of the community. When terrorist organisations invite them into the imaginary scenario with so-called ideals and goals completely opposite to the hidden ones, these individuals easily get trapped into the system.

Terrorist organisations use different motives to attract the attention of the target population. They use ethnic, social, religious and psychological framing to draw the attention of the individuals and the community.

On one side, the members of the terrorist organisation are called as terrorist by the majority of the community, on the other side they are called as heroes by some groups and regions. When the target population and region support them, it gives the organisation reasons and motivation to continue terrorist actions.

Particular events may ignite terrorism and increase recruitment efforts. An attack against a nation or a specific group, a declaration that threatens a specific nation, an action or simply perception of discrimination or humiliation or disrespect are specific examples that may trigger recruitment.

Additionally, the following root causes(5) are associated with leading to the emergence of terrorism and accordingly recruitment:

- Failed or weak states,
- Extremist ideologies,
- Historical roots of political violence,
- Hegemony or inequality of power,
- Repression by foreign powers,
- Experience of discrimination or social injustice.

### 4. Who Are More Suitable For Recruitment? What Are Common Characteristics? How Are The Recruit Candidates Selected Among The Target Group?

Various researches show that most

individuals who join terrorist organisations and become active members are mentally normal(6). Additionally, there is as of yet no identified universal terrorist personality pattern(7). However, statistics show that these individuals carry certain social, psychological and behavioral characteristics. They have an ideological way of viewing the world.

Examining new trends(9) will give us clues for future. Recent surveys indicate that education level of average terrorist is increasing. The universities serve as the recruiting ground. Moreover, several potential trends give considerable further warning. These include a general lowering of the entry age into terrorist activity, increased involvement by technically trained individuals, and increasing operational and leadership roles for women. These points indicate that terrorism is spreading dangerously.

When talking about new trends, we should also discuss the involvement of women. One of the motivations behind the recruitment of women appears to be the attempt to exploit the image of women, which raises less suspicion than men. The terrorist organisations also wish to take advantage of the sensitivity demonstrated by security forces, and their reluctance to carry out searches of their person. More contempting than these, women whose social standing is regarded as problematic have often been convinced to take part in terrorist operations as a means of rehabilitating their status in the society.

**5. What Recruitment Methods And Steps Are Applied?**

It has long been known that effective recruitment motives are tailored to the audience and its cultural, social, and historical context. Terrorist organisations apply different recruitment methods for different social groups and ages. Social, psychological and other relevant factors are all important because they increase the percentage of the population who support terrorism and therefore increase the pool of potential recruits.

Most terrorist organisations need to have a base region where they find supporters, sympatizers, financial support and safe havens etc. This area is vital to recruit new members, provide ideological, moral and political support and intelligence gathering. This base region should also reflect the feelings and the ideology of the terrorist organisation.

Therefore, terrorist organisations designate particular areas as their field for recruitment and concentrate on these locations with specific activities to prepare the population for their aims. They use both hard power and soft power to keep the area under their influence. Moreover, they prevent all state services and investments in the area using all means they have.

They use ajitation methods, psychological motives and various propoganda techniques to attract attention and gain sympatizers. They also use armed propaganda methods. This creates fear and increased pressure on the target population.

Accordingly, terrorist organisations designate individuals from the target region for recruitment and gather detailed information on them. The aim of information gathering is to find out what motivational factors will be more effective on each individual. They collect information on particularly the following areas;

- Family structure,
- Weaknesses,
- Friends he/she communicates,
- Economic level,
- Religious, ethnical and cultural root,
- Physiological, psychological and social needs.

After identifying the individuals ripe for recruitment, terrorist organisations employ various methods and means to recruit them.

**a. Social Means and Methods:** The use of social methods is quite common in recruiting new members. Terrorist organisations intensively use friend, family and relative relations; social and cultural activities; religious values and ethnical roots to influence recruit candidates. Recruiters exploit beliefs, relations, values and similar motives since most individuals are vulnerable to these motives in young ages. Terrorist organisations also use similarities and differences for recruitment and motivation effectively.

**b. Psychological Means and Methods:** Terrorist organisations use psychological

methods as well. They frame the individuals by influencing their psychology and penetrating into their perception. Since friends, family members and relatives are very effective on motivation and psychological pressure; terrorist organisations often employ these figures in combination for recruitment.

Terrorist organisations employ a gradual process for recruitment. This process consists of four basic levels as follows: Neutral, sympathizer, supporter, active member.

Neutralization of part of the population is important since this process reduces the number of the individuals against the terrorist organisation and facilitates propaganda and recruitment efforts. Sympathy can practically occur as a result of propaganda of the terrorist organisation or a negative action of security forces and government officials. In normal conditions, some of the sympathizers will turn out to be supporters with intensified pressure of the recruiters.

After all these actions, a triggering event or a similar cause may push the individual to decide to join the terrorist organisation. Later, this decision is supported by psychological framing, theoretical and practical training. The terrorist frames, motives and symbols are placed in the subconscious of the individual.

**7. Recruitment Models(10)**

There are tremendous varieties of recruitment models, but a review of the empirical studies on terrorist groups' recruiting reveals a few common structures. Social and psychological methods and other motivational tools are employed in these models in accordance with the conditions and requirements.

**a. The Net:** The audience who are viewed as homogeneous and receptive enough are approached in the "net" pattern (Figure 2). In this model, the candidates are engaged equitably and altogether. Some members will respond positively, others negatively; but in general the whole population is viewed as primed for recruitment.This approach is often used when there is little serious opposition to the group in the audience's environment.

**b. The Funnel:** Recruiters use the funnel model when they believe that the target population is ripe for recruitment, but requires a significant transformation in identity and motivation. As the term funnel implies, potential recruits start at one end of the process and are transformed into dedicated group members when they emerge at the other end. This approach can be characterized by brainwashing and group mindset building. Even individuals who fall out of the process can still be used as sympathizers.

**c. The Infection:** When the target population is difficult to reach, the terrorist organisations use the infection method. In this model, a trusted agent is inserted into the target population to influence potential recruits through direct, personal appeals. This method increases the persuasion and source credibility. As recruits proceed, the reach

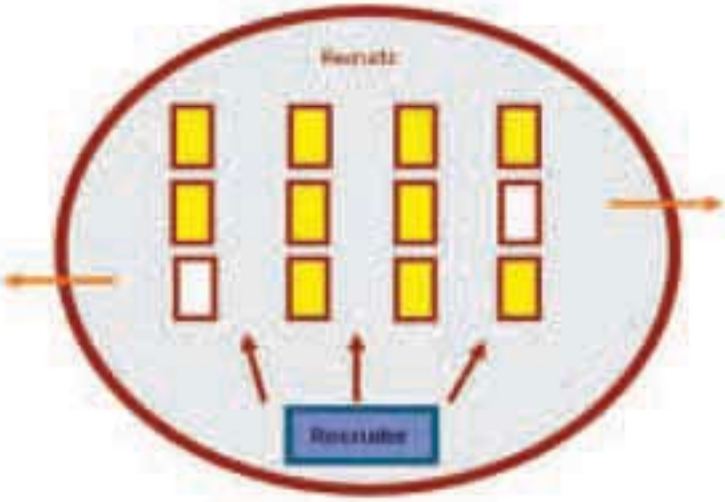



**Figure 2. The Net**

of the recruiting effort grows. However, this is an extremely time consuming effort. Infection is likely to be most successful in large governmental organisations such as the police or the military. An infiltrator may be able to convert selected members who are dissatisfied with their status and job.

d. **The Seed Crystal:** Often a target audience is so remote or so inaccessible that a trusted agent cannot be inserted into it. In this case, recruiters may seek to provide a context for self-recruitment such as Internet. Once individuals emerge within the population as new recruits, they will often follow the pattern of the infection. In terms of terrorist organisations, the seed crystal approach may be most successful in populations where open recruiting is difficult or impossible.

However, although almost all terrorist organisations use Internet effectively to reach their goals, the seed crystal is not considered as a secure recruitment model by most of the terrorist organisations since they have to operate secretly and they basically consider the individuals applying for membership on their own will as suspicious.

While Internet recruitment is very effective among sympathizers and individuals who are already primed to accept the organisations' message, it is mostly employed to propogate the

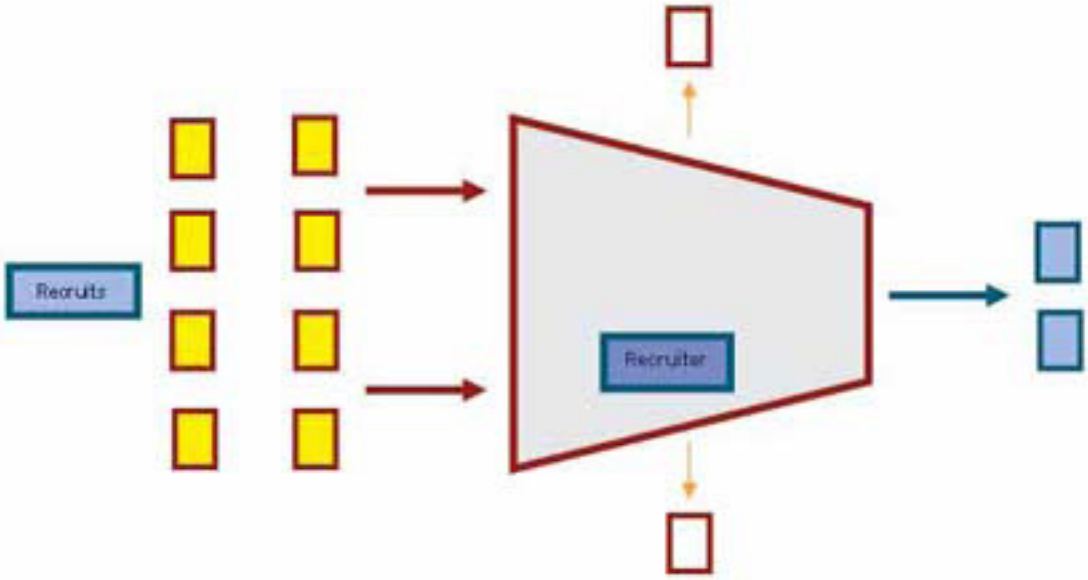



**Figure 3. The Funnel**

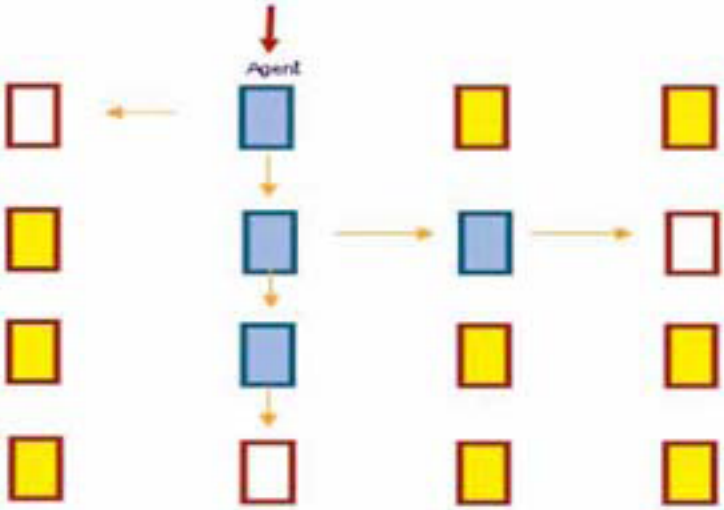



**Figure 4. The Infection**

ideology and strenghten the current membership.

**8. Post-Recruitment Process: Transformation From Thought To Action**

**a. Post-Recruitment Process:** Post-recruitment process is an extremely important step for terrorist organisations in order to transform the individuals from thought to action. They make up the terrorist identity through a series of transformation actions.

First, they build a wall between the members and the outer world by taking strict measures. With this thick wall, they prevent the individuals from communicating with their friends and families and following the mass media. By leaving the members alone within the selected group, they concentrate on the ideological framing, succeed brainwashing more easily and reach the desired effect in a shorter time.

Second, they apply an advanced ideological transformation by imposing their motives continuously. The aim of this process is to set a single way of thinking. This process is achieved by training, meetings, seminars and discussions formed by controlled questions and answers. Subsequently, disciplinary measures are imposed with a gradual increase and tolerance level is decreased in the same way.

In the next phase, the terrorist organisation assigns simple responsibilities to selected members to test their loyalty and adaptation and form the group mindset. These responsibilities are aimed at preparing the members for further tasks and actions. These are small group responsibility, publication responsibility, maintenance of equipment and so on.

The following phase is preparing the dedicated, ideologically framed and successful members for action. In the beginning of this phase, the members are given secondary tasks such as transportation of equipment and ammunition for action, watching, armed protection etc. Later, the members who are found decisive, cool and talented are encouraged and guided for armed actions and bombings.

With these phases, the terrorist organisation transforms the recruits' own personality into the group mindset(11) which can be described as a fixed mental attitude. Most of the time, this mindset will reflect their ideology and the personality of the leader.

**b. Group Formation and Dynamics:** As discussed before, terrorist organisations influence the members to maintain a single way of thinking in accordance with their ideology. This is vital for them because there is no room for individuality and uncontrolled behaviors in the organisation. Each member has to obey the organisation's functioning, stereotyped values and goals.

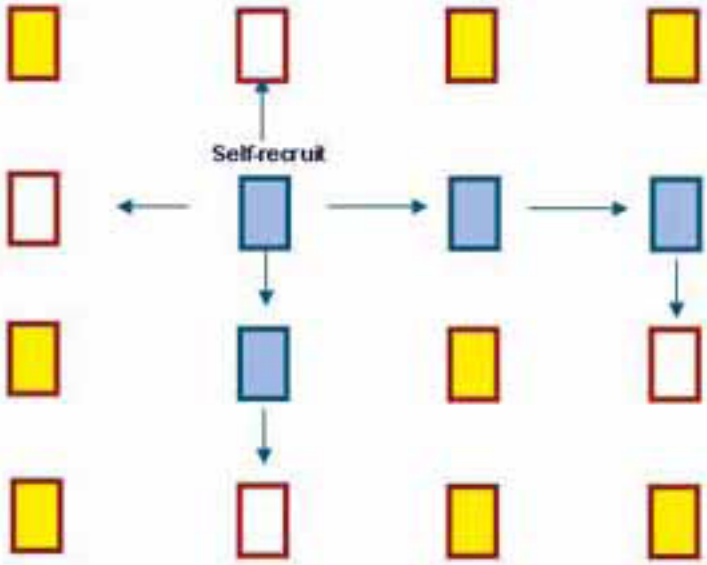



**Figure 5. The Seed Crystal**

Shared danger adds to the organisation as well and accelerates the group formation.

There is a solid hierarchic structure and chain of command in the organisation. Hundred percent cooperation and obedience is required at all times. They operate in "cell system" and actions are executed secretly. In the cell type structure, there is extremely limited contact among different groups. This system helps them operate covertly. No tolerance is shown for uncovering secrecy. To achieve this, they keep the new recruits under control by dedicated and experienced members through the recruitment phase and in the beginning of post-recruitment period.

Terrorist group dynamics point out a strong tendency to refuse the motives of the system. They reject alternative views, reflect a closed mind and are unwilling to compromise. They have tendency to see things in black and white.

Terrorist organisations apply completely different methods to keep the terrorists in the organisation when comparing with the recruitment process. While they apply motivational and soft techniques for recruitment, they use dominantly negative motives, fear and intimidation after recruiting the individuals. The motives such as freedom, equal rights etc. disappears and instead strict rules such as threat, fear apply.

After participating in the terrorist actions, the members are obliged to the organisation in two ways. The individual feels the intensive stress of group dynamics and rules from inside and the pressure of the security forces from outside. Individuals cannot leave the organisation on their own will. In other words, they do not have option to return to their regular lives. In such attempts, as a minimum, they are exposed to physical and psychological torture.

The psychological condition of a terrorist organisation member might be described with learned helplessness theory(12). Learned helplessness is a psychological condition in which a human being has learned to believe that he is helpless and has no control in a particular situation. As a result, the individual stays passive in the face of an unpleasant, harmful or damaging situation, even when he actually has the power to change the conditions. A test applied on dogs provides remarkable results. They place several dogs in a cabin and keep the gate open. They exert low electrical shock to all dogs and when the dogs feel uneasy, they try to go out of the cabin using the gate. As one dog arrives to the gate, they exert higher electrical shock and the dog returns back to the cabin. After they repeat this test for some time, dogs refrain from the gate and stay inactive. Although they cut the electrical shock at the gate and exert it inside the cabin, the dogs do not try to go out and stay inside. This learned helplessness test may be a good example for the psychological conditions of the terrorists inside the organisation.

**9. Countering Recruitment**

It might be interesting to start discussing countering recruitment with a specific question. Does counter-terrorism breed more terrorism? Today, hard power(13) is intensively used for countering terrorism. However, these measures are applied not only on terrorist organisations but also on the communities. From different examples around the world, we can infer that hard power which is not blended with soft power or directed to the wrong address worsens the situation and breeds more terrorism.

Countering recruitment is key to success in defence against terrorism. Use of force is an important measure, but not sufficient alone to counter terrorism. There is a common expression: "Instead of fighting against the mosquitos, try to dry the swamp." By the time you kill or arrest one, several others may appear in the scene.

Countering recruitment in schools, social activity centers and worship areas is essential. However, it doesn't mean to conduct continuous operations to these types of facilities. If an illegal activity is detected in these areas, there are various ways to counter it other than conducting an immediate operation. We should think that while seizing a few terrorists, we might help recruitment of several others.

Researches(14) clearly demonstrate that prisons are extremely convenient for recruitment efforts. One of the so-called leaders of PKK terrorist organisation

declared that Diyarbakır Prison Facility was the hearth of the organisation in the establishment process(15). A research(16) conducted in another terrorist organisation reveals that nearly 70 percent of the recruits were arrested or sentenced before joining the organisation. These examples dictate the clear requirement of countering the recruitment efforts and ideological propaganda activities in the prisons. Psychological treatment, counter-ideological rehabilitation, continuous inspection and observation are required to maintain recovery from terrorism and prevent recruitment efforts.

Security forces should conduct counter terrorism operations successfully and take effective security measures against terrorist activities because successful terrorist acts, particularly attacks to the targets selected and slandered by the terrorist organisations trigger recruitment. Terrorist organisations feed on terrorist events and destruction. However, counter-terrorist actions can be successful if the separation of the terrorist organisation and the local population can be made distinctively. You may be sure that the idea they have in their mind is wrong and even provoked and misled by the terrorists, but immediate refusal and use of force against the community may produce negative reaction. In fact, these measures may facilitate the goals of the terrorists. Here, it is important to highlight that while the use of force against the terrorists supports counter-terrorism efforts, the use of force against the whole target population or trying to identify terrorists from some common characteristics instead of using concrete evidences may facilitate recruitment.

Another counter-measure to recruitment is intelligence. Aggressive intelligence activity is important to track the activities of terrorist organisations and monitor developments. Community involvement and interaction between moderate target population and the authorities is critical to success.

As terrorist organisations deal with human, drug and weapon trafficking, they continuously raise funds and this makes terrorism attractive. Therefore, international cooperation should be established to fight against the financing of terrorist organisations.

Recruitment is clearly the lifeblood of terrorist organisations. However, it is a fact that authorities are not concentrating sufficiently on diminishing recruiting, but on trying to stop attacks. Both are important, but understanding how recruitment mechanisms in different regions function and addressing them correctly will help diminishing terrorism.

Considering that individuals are exposed to a very long transformation process through becoming a terrorist, it is extremely difficult to disengage members from the terrorist organisation. Terrorist organisations recruit individuals and transform them into a terrorist. Our primary goal is to prevent them from joining the terrorist organisations because it is very difficult, if not impossible, to transform a terrorist into a normal individual. "They are making sausage from the cow. We need to stop this sausage–making process at the beginning. Otherwise, it will be quite challenging to make a cow from the sausages."

Counter-recruitment activities and measures should be implemented in accordance with a well-prepared plan which includes legal, social, psychological and economic measures. Terrorist organisations select their recruitment area from the regions where education, economic level and social conditions are quite low. Therefore, messages for counter-recruitment should be understandable and acceptable in these areas.

Education level is associated with the literacy rate and illiteracy is seen as a social problem to be solved through education in many countries. However, when examining the definition of literacy(17) and the conditions deeply, this calculation is not sufficient for correct decisions. In many countries, educational activities do not support and increase literacy level of the individuals satisfactorily. Actual education level can be considered enough if this level helps understanding and proper reasoning of the individual.

In underdeveloped countries and in other countries that have underdeveloped regions, the actual education level is extremely lower than the desired level. Social and economic conditions are quite similar to the education level. Improving education, social and economic level of the target populations will facilitate counter-recruitment activities.

Another problem to work on is high population growth rate in target areas. Let's remember the figures provided in the beginning of the discussion. It is a fact that high birth rate produces negative effects in chain reaction in particularly developing and underdeveloped countries. In developed countries, the birth rate per women is around one while it goes up to 7 in some parts of the developing and underdeveloped countries(18). With high birth rate and low income level, satisfying the basic needs of the population is extremely difficult. However, it is also very difficult to solve this problem in a short time. Authorities should focus on this problem and with the help of education, training and campaigns; this rate should be lowered gradually in such regions. Although long term effort is required, the solution of this problem will reduce terrorist recruitment.

Emphasizing family values is another key requirement for countering recruitment. Terrorist organisations are aware of the importance of the family values and for this reason they try to prevent their members to communicate with their families. Turkish authorities has initiated a campaign(19) and established a close cooperation with the families of the individuals who were trapped by the terrorist organisations. As a result of this campaign, a significant number of the terrorists disengaged from terrorism.

Another cause for recruitment is triggering events, discrimination, humiliation and mistreatment of authorities and security forces. The region may be a field for recruitment and full of sympatizers; however, reacting to all population as potential terrorists will cause negative and triggering effects. Positive attitude will flourish positive outlook and mutual understanding. Let's give an example(20) from Turkey. There was a demonstration in one of the cities in eastern part of Turkey and the terrorist organisation provoked the population for aggresion. They provoked the children, placed them in front of the group and instructed them to throw stones to the police. The children threw stones to the police but the police reacted in a very different way. While defending themselves with shields, they started to distribute bananas to the children. The children stopped throwing the stones and ate the bananas. Of course, this may not be applicable in every occasion. However, it was a symbolic action and a good message to the children and the group. "We understand that the terrorist organisation is trying to provoke you but we believe you are not supporting them. You are our citizens and we see you as our own kids." On the other hand, let's consider what could have happened if the physical force had been used against the children. It could stop them at that moment, but could also cause provocations and be used in propaganda and recruitment efforts.

Another point to discuss is similarities and differences. By respecting different cultures and religions, these motives should be taken back from terrorist organisations. Messages and efforts must promote civilization symbols such as understanding human rights, better way of life and living standards etc.

Similar positive messages should be used to counter ethnic terrorism as well. Instead of refusing the strong ethnic beliefs of the population, counter messages should focus on understanding the difficulties and problems the target populations have faced. We don't have to and cannot agree with all claims, but understanding that direct refusal of claims brings resistance in the population, we should proceed through a well-organized plan considering all aspects such as educational, social, psychological and economic recovery. Terrorist organisations struggle and put the table all the points for the target population to feel themselves different, why don't we try to tell them similarities.

If the terrorist organisation address the feelings and influence the perception of the target population, then they will increase the number of the sympatizers and recruit new individuals. "If the weather is cold and the ground is similarly icy, the snow will accumulate, if not it will melt."

Knowing the mindset of the terrorist group will enable the counter-terrorism efforts within the target population. Counter-recruitment efforts should focus on this point and try to address the perception of the population more intensively than the terrorist organisation.

The terrorist organisations have many actions and thoughts that contradict their claims and the facts. These points can be used effectively for counter-recruitment efforts.

- They claim that they are struggling for freedom and equal rights but they run the organisation with a fear and intimidation policy.
- They claim that the target region is poor and not developed but they destroy the infrastructure and the facilities.
- They claim that they struggle for their culture and values, but they kill their own people.

**10. Conclusion**

Considering the recruitment methods and counter measures, the following arguments will arise: First, there is no single, uniform recruitment process for a group; rather, there are as many recruitment processes as there are distinct regions in which different groups operate(21).

Second, and correspondingly, the recruitment efforts of a group will not be mitigated, hindered, or halted by a one-size-fits-all prescription(22). Different regions and cultures will necessitate different counter-recruitment efforts. Additionally, as the recruitment methods of terrorist organisations differ, counter-recruitment efforts for each case may also require different methods. While some counter-recruitment methods might be effective in some regions, they might not produce positive results in some other areas.

Trends in terrorism and recruitment efforts should be examined continuously. By the time, one recruitment method is identified, terrorists invent and operate another. Counter measures are mostly a 'response' to the terrorist activities, thus terrorists always seem to be one step ahead. This is an important to fact to bear in mind in the fight against terrorism.

**References**

*(1) "World Development Indicators", World Bank Report, 2008.*
*(2) "United Nations World Population Prospects: The 2006 Revision", Population Newsletter, No:83, June 2007)*
*(3) COE-DAT Annual Terrorism Report, 2007 (Number of Terrorist Events/Country).*
*(4) Abraham Maslow, A Theory of Human Motivation, 1943.*
*(5) John Horgan, The Psychology of Terrorism, 2005.*
*(6) Martha Crenshaw, The Psychology of Terrorism, 2000; Rex A.Hudson, The Sociology and Psychology of Terrorism, 2005, p.26-31.*
*(7)Walter Reich, Understanding Terrorist Behavior, Origins of Terrorism, 1998.*
*(8) Samih Teymur, An Analysis of Terrorist Recruitment, August 2004.*
*(9) Raphael Perl, "Trends in Terrorism:2006", US Congressional Research Service, July 2006*
*(10) Scott Gerwehr-Sara Daly, "Al Qaida: Terrorist Selection and Recruitment", RAND Corporation.*
*(11)Rex A.Hudson, The Sociology and Psychology of Terrorism, p.26-31, 2005.*
*(12) International Terrorism and the Drug Connection, Ankara, 1984, p. 148-151, Origin: Martin Seligman, 1975.*
*(13) Joseph S. Nye, Soft Power: The Means to Success in World Politics, 1990*
*(14) "Terrorists: Recruiting and Operating Behind Bars", US Directorate of Intelligence, August 2002*
*(15) Master Thesis on PKK/KONGRA-GEL Terrorist Organisation, Ankara, 2005.*
*(16) Samih Teymur, An Analysis of Terrorist Recruitment, August 2004.*
*(17) UNESCO Definition: "Literacy is the ability to identify, understand, interpret, create, communicate, compute and use printed and written materials associated with varying contexts. Literacy involves a continuum of learning to enable individual to achieve his or her goals, to develop his or her knowledge and potential, and to participate fully in the wider society."*
*(18) United Nations, Department of Economic and Social Affairs, Population Division, World Fertility Patterns 2007.*
*(19) Fikret Bila, Milliyet Newspaper Article, 2008.*
*(20) CNN Turk, February 2008.*
*(21) Scott Gerwehr-Sara Daly, "Al Qaida: Terrorist Selection and Recruitment", RAND Corporation*
*(22) Scott Gerwehr-Sara Daly, "Al Qaida: Terrorist Selection and Recruitment", RAND Corporation*

# Terrorism as a System

**Erdoğan ÇELEBİ**
*Captain (TUR A)*
*COE-DAT*

## 1. Introduction

The open system framework comes from the "general system theory" of Ludwig von Bertalanffy in the 1940s. Daniel Katz and Robert Kahn introduced the open system theory in their seminal work, the *Social Psychology of Organizations(1)*. Since then this interdisciplinary framework of organizations replaced the old limited structural approach.

Open system theory views organizations as systems interacting with the environment, or in Ludwig von Bertalanffy's words "organized cohesive complex of elements standing in interaction(2)." The interaction refers to both the relationship between a system and its environment, and among the complex elements o the system (subsystems). Subsystems perform the specific functions required for organizational survival, such as production, boundary spanning, maintenance, adaptation, and management(3). Organizations' survivability depends on the proper and aligned functioning of these subsystems.

Systems inherently are exposed to entropy- a term originated in thermodynamics- which means the tendency for systems to move forward to a chaotic or random state, in which there is no potential for energy, transformation or work. "Organism" is a metaphor for organizations which grow, adapt, spawn and sometimes die. At other times their existence is due to negative entropy (store of energy, winter fat of the organizations(4)), by which organizations may live indefinitely. An organization's effectiveness and success depends heavily on its ability to adapt to its environment, shape the environment, or find a favorable environment in which to operate(5).

All open systems have the following basic characteristics:
1. They import energy and resources from the environment (input)
2. They transform this energy and resources (throughput)
3. They export the product to the environment (output)
4. They adapt their components in a dynamic pattern of activities (feedback).

## 2. Terrorism as an open system

Terrorist systems are open social systems importing the inputs (people, money, weapon, and information etc.) into the transformation process to export the output (fear, terror, intimidation, awareness, coercion, mobilization) into the environment again to achieve the organization's primary task. The feedback mechanism enables the organizations to adapt to an unstable environment; also, it allows the subsystems to work in

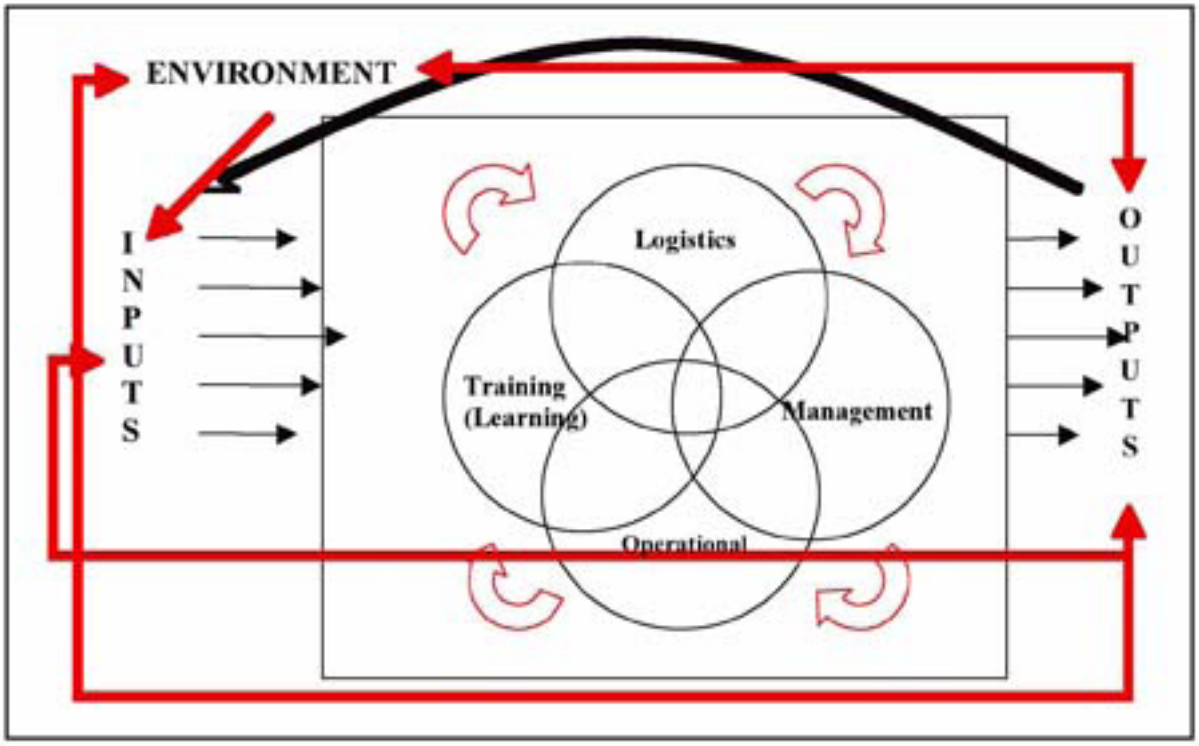



**Figure 1. Terrorism as a System**

alignment with each other.
Previous studies about terrorism and counterterrorism were compartmentalized into some specific categories such as psychological, environmental, organizational or instrumental. All the components of the terrorist system (inputs, outputs, environment, and subsystems) are very interrelated. In order to explain terrorism and terrorist organizations in systems terms, first we have to understand these components and the relationships between and among these components. These relationships are not constant but dynamic. The dynamic nature of these relationships is a power of dark organizations in terms of their adaptation to their environments.

**3. Relationship Between Environment And Use Of Terrorism (Outputs)**

There are plenty of studies explaining the relationship between environment and use of terrorism and the emergence of terrorist organizations. The primary effect of the environment to the terrorist organizations is that environment has a preparatory effect on individuals (input) to participate in the terrorist organization.

The environment in which terrorist organizations operate consists of target audiences from which the organization seeks support, other rival organizations that have the same goal, counter terrorism organizations that add more turbulence to the environment, and social, political and economic conditions.

Ted Robert Gurr observes that there is a relationship between economic disparity and the tendency of individuals to resort to violence, and he generalizes this disparity with the term "relative deprivation." Relative deprivation is the discrepancy between the "ought" and the "is" of collective value satisfaction(6). One of the main pillars of his approach is how long the group is subjected to feelings of deprivation and the extent to which it believes things may change. The longer that deprivation persists, combined with the subjective feeling that chances of change are small, the inclination to violence will grow(7).

Krueger and Maleckova argue that the evidence they presented in their study suggests that there is little direct connection between poverty, level of education, and taking part in terrorism. Their analyses of datasets about Hezbollah members and Palestinian suicide bombers show that they come from economically advantageous families, and they have relatively high levels of education compared to the general population(8).

The 9/11 Commission report reached a similar conclusion: "Terrorism is not caused by poverty. Yet when people lose hope, when societies break down, when countries are fragmented, the breeding ground for terrorism are created(9)."

A causal relationship between economic systems in the environment and terrorism is another subject that was studied by Michael Mousseau. He argues that there is a contract based relationship between people in liberal democracies and a clientalist relationship in authoritarian societies, and the economic integration of the society has a great effect on terrorism:

*Social integration with contracts promotes respect for individual choice, the equal rights of strangers, and religious and cultural tolerance: the cultural base of the liberal state. Social integration with reciprocity promotes acceptance of the group beliefs and values, loyalty to the group leaders and distrust of outsiders: the cultural basis of authoritarianism and sectarianism. In this way, a socio-economy of reciprocity is a necessary condition for the resort to terror and genocide and a leading cause for illiberal democracy, ethnic separatism, and weak and failed states in the developing world(10).*

Thinking of the results of the studies, which concludes that the majority of the terrorists come from wealthy or middle class families, and the reality that people become more engaged politically and ideologically when they reached a fairly high standard of living, and that terrorism is the most extreme form of political engagement, one wonders if wealth is the reason. Daniel Pipes argues that "the spread of free market capitalism and liberal democracy . . . is probably an important factor in rising political Islam(11)." The main pillar of his argument is that wealth, freedom of speech, and representation of extreme ideas that are offered by capitalism and liberal democracy in the Middle East also creates sources and opportunity for radical movements.

Another popularly argued theme is the correlation between the democratic conditions in the environment and terrorism. F. Gregory Gause III argued that there is little data to support the notion that democracies directly diminish the prospect of terrorism(12). Citing the survival of ETA after Spanish transition from dictatorship to democracy, the IRA in the UK, one of the oldest democracies, terrorist attacks in India, the world's largest democracy, the Red Army faction in West Germany, and the Oklahoma City bomber, Gause demonstrates that democracies are equally susceptible to terrorism. On the other hand China, an authoritarian state, had no terrorist incident reported in State Department's Patterns of Global terrorism report(13). As Dr. Michael Freeman concluded, democracy may be a cure for tyranny but not a good cure for terrorism.

Erica Chenoweth looks at the environment from a government stability perspective. According to Chenoweth, levels of democracy do not necessarily diminish the likelihood of terrorist development(14). Instead, the political stability of the existing regime is the most significant factor affecting the origins of terrorism. She argues that the results in her study appear to show that governments should crack down on terrorism and revoke civil liberties in order to maintain stability, but defeating terrorism is not always the desired outcome. Implying state repression and state terror, she concludes that "stability, no less than revolution, may have its own kind of terror(15)." How the government of Peru's struggle and achievement against Shining Path turned into a tool of eliminating political rivals and consolidating the tyrannical power of Fujimori is an apt example to show the need for separating terrorists from the population in the efforts of counterterrorism(16).

The effects of other rival organizations in the environment are another relationship between an organization and the degree of terror that the organization may employ. Mia Bloom argues that if there are similar organizations in the environment it is likely that the violence will escalate as a result of rivalry among the groups. She supports her argument by giving examples from three Palestinian groups Al-Aqsa Martyrs Brigade, Palestinian Islamic Jihad and Hamas(17).

**4. Relationship Between Outputs And Environment**

The outputs of terrorist groups are basically creating fear and a sense of insecurity, intimidation, mobilization of the population around their cause, awareness (propaganda by the deed), and coercion of the government until they reach their goals.

The effects of the outputs of terrorist systems on an environment or population were studied by Friedland and Merrari in a survey on the Israeli population about their willingness to concede to terrorist

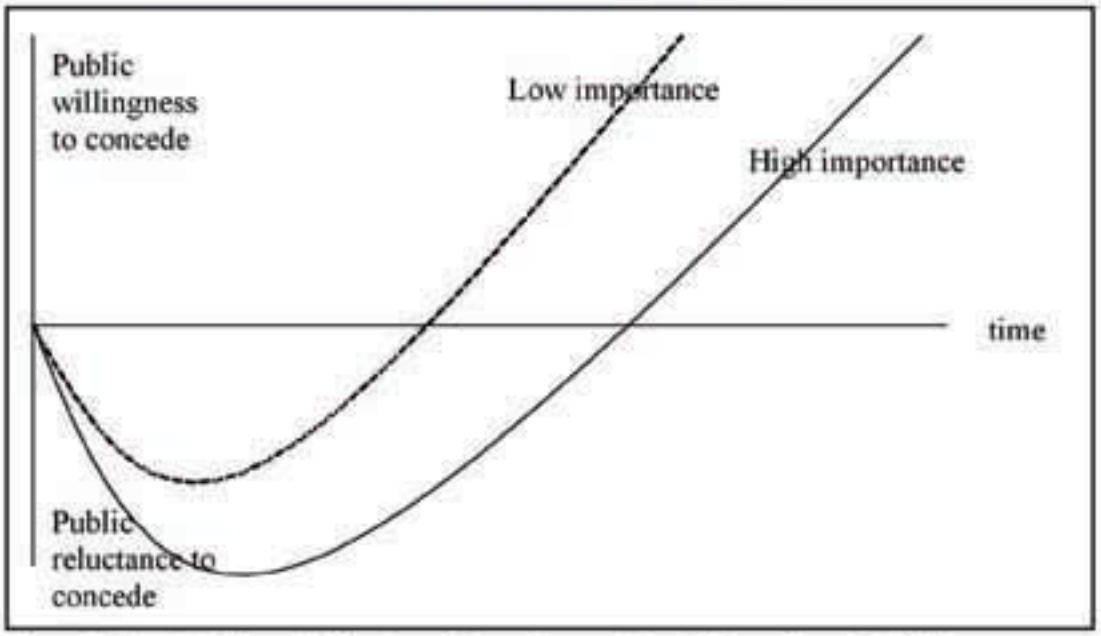



**Figure 2. The Relationship between Importance, Threat Intensity and Public Willingness to Concede to Terrorist Demands**

demands(18).
According to their study, during early stages the terrorist threats can lead to a strengthening of public resolve not to concede. The extent and the degree to which such strengthening might occur is related to the importance of the issue to the public; the more important the issue, the greater the strengthening of resolving not to concede in the face of the threat. However, the more prolonged the threat, regardless of the importance of the issue, the greater eventually is the probability of conceding to the terrorist demands. The importance of the subject to the public is in relative terms, and the importance of the same issue may be perceived differently in various societies. The secessionist demands of ETA and the importance of the issue in the minds of Spanish people compared to the same demands of terrorist organization PKK and the importance of the issue in the Turkish public's mind are relatively different. Consequently, Spanish people seem to be satisfied with the autonomy given to the region by the Spanish government. On the other hand, the Turkish public is unwilling to appease terrorist PKK's demands, although almost everyday a terrorist incident occurs in the country.

**5. Relationship Between Outputs And Inputs**

The output of the terrorist system is communication with the environment, what Gordon McCormick calls "signaling strategy(19)." Terrorist plots are a message to intimidate the enemy as well as a message to their support (and prospective support) groups that they are strong enough to challenge the enemy's superior power. The fear and insecurity they create in a population's mind leads the population to think that their security forces are not capable of providing the services that they are supposed to; thus there is more cause for the population to support the terrorist organization. Without support a terrorist organization cannot survive. To enable recruitment and logistical support, they have to demonstrate enough violence or terrorism, which they see as "propaganda by deed." The money that they make from the terrorist acts like extortion, bank robberies, and drug trafficking is funneled back as an input to sustain the organization. As a result the outputs of the terrorism system attract or try to mobilize the population to support the terrorist organization and its cause.

Not only outputs affect the inputs, but also inputs have effects on the outputs. The terrorist organizations try to recruit very selectively according to distinct criteria which will be discussed in detail in next chapter, because the wrong people may cause adverse consequences for the terrorist organization.

**6. Interrelations Between Subsystems**

Systems must overcome the universal law of nature in which all forms of systems move toward disorganization or death. Congruence, sometimes referred to fit or alignment, is a prerequisite for systems to operate efficiently. Congruence is defined as the relations among the internal system components and between systems and their environments(20). As suggested in Figure1, terrorism system is composed of four subsystems that fulfill the necessary functions. These subsystems are dependent on each other, and one's dysfunction can cause the entire system to collapse.

The training subsystem recruits from a population, equips the recruits with necessary mindsets and skills, and enables the system to adapt to the hostile environment by means of organizational learning. Social organizations, because they are open systems, can import more energy from the environment than is immediately required and store it for use during periods of crises such as a concentrated counter-terrorism campaign. This process is called negative entropy. Unless the negative entropy capability is shattered the terrorist organization will survive. The training subsystem is the main creator of negative entropy.

The operational subsystem is responsible for directly producing the outcomes of the terrorist system, which is very important for its survival. As Gordon McCormick writes, "Terrorist groups must maintain a minimum violent presence to remain effective. . . To hold their audience (and hold themselves together) they must continue to act(21)."

The logistics subsystem is responsible for providing necessary resources that other subsystems need to fulfill their functions. This subsystem is the closest subsystem to the environment from which the

terrorist organization is fed, so this subsystem must act in very clandestine manner in order to maintain its legitimacy in the eyes of its population and the government. Also the distinction between the sympathizers and active members of the terrorist organization blurs in this level in terms of counterterrorism activities. Security forces have to be ready to confront the problems posed by this blurry situation in their efforts not to play into the terrorists' hands, who try to provoke overreaction of the government.

The management subsystem is responsible for decision making, strategy development, and exercising control or influence over the organization. The influence and control over the organization changes from group to group, based on ideology and counterterrorism measures, but the coordinator role of this sub-system is common in all terrorist organizations. PKK is an example of a highly hierarchical terrorist organization as a result of its Marxist Leninist ideology that sees the organization as a vanguard of the alleged movement; on the other hand, Al Qaeda is at the other extreme--franchising terrorism around the world with terror entrepreneurs. However, both core management subsystems approve and coordinate the terrorist actions.

**7. Conclusion**

Terrorist systems are complex open systems that have some unique characteristics, as stated by Virginia Anderson and Lauren Johnson(22):

*1. Complex systems tend to be self stabilizing*
This characteristic explains why so many terrorist organizations still exist although there is enormous efforts to stop them functioning. They mutate to fit their environment; first, to survive, and second, to achieve their goals.

*2. Complex systems are or appear to be purposeful*
Terrorist systems stabilize themselves by means of various strategies that may appear to be in conflict with the organization's overall goal. However, it is purposeful, because the terrorist organizations use various reinforcing loops--loops compound change in one direction with even more change in that direction--that are aligned with the overall goal of the systems, but also some balancing loops—loops or interventions to the system that try to bring things to the desired state and keep them there--that appear to be conflicting. For example, terrorist organizations want as many members as possible, but this endangers the underground nature of the organizations and makes them susceptible to destruction by counter terrorism agencies; thus they use a balancing loop to decrease the active membership for survival, especially in the initial stage.

*3. Complex systems, like simpler systems, are capable of using feedback to modify their behavior*
The self stabilizing function is achieved by a feedback mechanism between all the components of the system. The operational subsystem arranges levels of violence according to feedback that comes from the environment (population). The logistics sub-system sends feedback to the management subsystem to find new methods for maintaining financial support. The training subsystem arranges itself according to the feedback that comes from the increasing pressures of counterterrorism agencies, and finds new ways to recruit and train its members.

*4. Complex systems can modify their environments*
The main goal of terrorist organizations is to modify their environments, simply because they are not pleased with the current environment, be it the economic system, constitutional conditions or current territorial structure of the country. Unlike other lobby organizations, they try to change it by violence.

*5. Complex systems are capable of replicating, maintaining, repairing, and reorganizing themselves.*
Al Qaeda is an example of how a terrorist organization replicates itself. It began with a hierarchical structure, and now no one knows exactly what it is--an organization, a network, a movement, or a global insurgency.

After explaining how terrorism destabilizes its environment in system terms, it must also be noted that systems thinking can also be used to destabilize terrorist organizations; the choice is up to the time, tolerance of the consequences of the choices, and decisiveness of the choices. These choices would be to cut the energy that the system imports (i.e., financial support); misaligning the one or more sub-systems (i.e., the training subsystem); creating a turbulent environment that they can not tolerate

(overwhelming control over the environment, i.e., increasing troop numbers); changing the environment in a way that it can not affect the inputs to resort terrorism (bring democracy to the Middle East, because democracies don't fight each other); or change the environment in a way that the outcomes of the terrorist organization can be absorbed or tolerated by the environment, and do nothing (more people die in traffic accidents than do in terrorist plots). All these alternatives come with their own side effects that counter terrorism agencies must consider and make tradeoffs.

**References**


*(1)Troy S Thomas at al., Warlords Rising, (New York: Lexington Books,2005) p.11*
*(2) Ludwig von Bertalanffy, 1976, quoted in Troy S Thomas at al.', Warlords Rising, (New York: Lexington Books,2005) p.11*
*(3) Richard L. Daft, Organization Theory and Design (Mason , OH: Thomson South Western, 2004),14*
*(4) William D. Casebeer, quoted in Troy S Thomas at al.', Warlords Rising, (New York: Lexington Books,2005) p.16*
*(5) Daft, p.15*
*(6)Ted Robert Gurr, Why Men Rebel (Princeton NJ: Princeton University Press, 1970)*
*(7)Scot Atran, "Mishandling the Suicide Terrorism", Washington Quarterly, p. 77-79*
*(8) Alan B. Kruger and Jetka Maleckova, "Poverty, Education and Terrorism: Is there a Causal Connection?", Journal of Economic Perspectives, 17, Fall 2003, p.119-144*
*(9)Quoted in Yonatan Levy, "9/11 Report: The Middle East Dimension", available at http://www.washingtoninstitute.org/distribution/Pol890.doc accessed 13 September 2006*
*(10)Michael Moussean, "The Nexus of Market Society, Liberal Preferences, and Democratic Peace: Interdisciplinary Theory and Evidence," , 47, December 2003, pp. 483-510*
*(11) Daniel Pipes, "God and Mammon: Does Poverty Cause Militant Islam?", National Interest, 66 Winter 2001/2002 , p. 14-21*
*(12) F. Gregory Gause III, "Can Democracy Stop Terrorism?," Foreign Affairs, September/October 2005*
*(13) US State Department, "Country Reports on Terrorism, East Asia and Pacific, China" available at http://www.state.gov/s/ct/rls/crt/2005/64336.htm accessed on 13 July 2005.*
*(14) Erica Chenoweth, "Instability and Opportunity: The Origins of Terrorism in Weak and Failed States" in The Making of a Terrorist ed. James J. F Forest, vol.3 Root Causes, (Westport CT: Greenwood Publishing Group, 2006) p. 17-31*
*(15) Ibid. 21*
*(16) "State of Fear: Peru's Comisión de la Verdad y Reconciliación," DVD, New Day Films*
*(17) Mia Bloom, Dying to Kill: the Allure of Suicide Terror, (New York: Columbia Uni. Press, 2005)*
*(18) Friedland and Ariel Merrari, cited in Maxwell Taylor, The Terrorist, ( New York: Brassey's Defense Publishers, 1988 ), p.29*
*(19) Bruce Hoffman and Gordon McCormick, "Terrorism, Signaling and Suicide Attack," Studies in Conflict and Terrorism, 2004,27, p. 243-281*
*(20) Michael I. Harrison and Arie Shirom, Organizational Diagnosis and Assessment: Bridging Theory and Practice, (Thousand Oaks, CA Sage Publications), 1999, p.52*
*(21) Hoffman and McCormick, p. 245*
*(22)Virginia Anderson and Lauren Johnson, Systems Thinking Basics, (Massachusetts: Pegasus Communications Inc., 1997), p.78-79*

## COE-DAT Activities

1 COE-DAT organized a **NATO Advanced Research Workshop** on "Transportation Security Against Terrorism" on 05-06 May 2008 in Ankara/Turkey. Focusing on the importance of transportation security in terms of terrorism, the workshop scrutinized the security of transportation routes and vehicles, terrorist risk for public transportation systems, the legal framework for defending transportation systems, the role of international organizations, particularly United Nations (UN) and European Union (EU) in transportation security, the intelligence and cyber dimensions of transportation security, future projections and protective measures for transportation security against terrorist threat. There were 64 participants from 20 different countries and 20 speakers from 9 different countries

2 COE-DAT conducted a **course** on "NATO Homelands Defence and Multinational Cooperation Against Terrorist Threats" on 26-30 May 2008 in Ankara/Turkey. Throughout the course, the root causes of terrorism, the concept of homeland security, the threat assessment in homeland security, terrorism in the homeland security, strategies for countering terrorism within homeland security and the elements of international cooperation in the fight against terrorism were dealt with. 31 participants from 12 different countries participated the course whereas 12 speakers from 7 different countries gave lectures.

3 COE-DAT carried out the **course** on "Countering Crowd and Riot Events Including Terrorist Activities" on 09-13 June 2008 in Ankara/Turkey. The terminology of crowd, riot, insurgency and terrorism is examined. In addition, the general characteristics of groups, crowds and psychology of the masses, the connections and separation between terrorism and insurgency were elaborated

Planning for crowd and riot control, the legal framework and principles for crowd and riot with particular reference to human rights and rules of engagement, techniques and tactics to disperse crowds were explored. There were 41 participants from 14 different countries and 10 speakers from 3 different countries.

## "Use of Force in Countering Terrorism" ATC

4 COE-DAT is organizing a **NATO Advanced Training Course** on "Use of Force in Countering Terrorism" on 08-12 September 2008 in Bishkek/KYRGYZSTAN. The course is designed to enable NATO specialists to share their expertise on terrorism and the use of force under the United Nations (UN) Charter in consistent with the right of self defence with trainees from a NATO Partner country. By this way, it is intended to assist the improvement sharing of information especially with and among Partner countries and identify problems which are particular to the Partner countries in the use of force in countering terrorism. The issue of the use of force in countering terrorism with reference to international law, human rights, law of armed conflicts, rules of engagement, the roles of UN and NATO will be elaborated via lectures, case studies, working groups and panel discussions.

## "Defence Against Suicide Bombing" Course

5 COE-DAT will conduct a **course** on "Defence Against Suicide Bombing", on 22-26 September 2008 in Ankara/TURKEY. This course has been conducted twice a year since the year 2005. The course is designated to analyze the issue of suicide terrorism with reference to the psychological, social, legal, financial, and intelligence aspects and also the preventive and countering strategies. The human component of suicide terrorism, the motivation, rationale, recruitment strategies and modus operandi of suicide bombers will be discussed. How to prevent suicide terrorism, identifying and detecting suicide terrorists, and the contributions of the international organizations to countering suicide terrorism will also be elaborated.

# COE-DAT

**Centre of Excellence**
**Defence Against Terrorism**

PK.57, 06582 Bakanlıklar
Ankara / TURKEY

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

www.coedat.nato.int

© **COE-DAT 2008** All Rights Reserved