NEW TECHNOLOGICAL OPTIONS IN PREVENTING AND OPPOSING INTERNATIONAL TERRORISM

Ion BĂLĂCEANU

Hyperion University, Bucharest, Romania.

Abstract: *The performance of today's computing environment has been transferred to the competition state and non-state actors in the field of military power to an broader coverage area, meaning the civilian sectors, exposed to risks and threats posed by international terrorism expansion. This article highlights the magnitude and consequences of terrorist actions in the civilized world and detailing some aspects of novelty in the field of computer technology in identifying terrorists, preventing and combating terrorist acts.*

Keywords: *terrorism, counter-terrorism policy, information technology, biometrics, special operations*

1. TERRORISM – THE UNPREDICTABLE ENEMY OF THE CIVILIZED WORLD

The civilized world has a new treacherous opponent, unpredictable and extremely dangerous - terrorism. Faced with the evolvement of this subject, the effects and consequences of it, threatening the very existence of universal human values, the international community more united than ever, triggered a battle without equal "evil forces" with germs and its vectors. The worsening of terrorism in general, and the manifestation, in particular, have been possible under the contemporary security environment. Given its coordinates, we appreciate that terrorism has become, at present, a transnational public problem.

More and more obvious is that significant actors on the contemporary world scene are not only state actors but also some multinational companies, humanitarian organizations, agencies, groups and even individuals, all of them enrolling in the ubiquitous process of globalization. Among other things, globalization has allowed unrestricted access to information. The imformation, used and targeted in a particular way, it becomes a generator of instability and insecurity involving various forces and means whose sizing can sometimes be considerable.

Thus, under these conditions, with relatively low costs, it is quite easy for those interested to pose a threat. Therefore it is possible that the movements (of any kind), including terrorism, to have access to high-performance technology, weapons and modern weapon systems.

Therefor, the use in specific terrorist actions of a very wide range of mediums, techniques, tactics and procedures is no longer a burden. Because of that, the organizations and terrorist groups widened and diversified their purposes, making the risk even greater. In essence, they can vary depending on the objectives that the terrorist groups may pursue and may relate to:

-alerting public opinion and political power of terrorist groups and detailed explanation of its requirements;

-demonstrate the power and paralel operating mode regarding the government vulnerabilities targeted by an terrorist group;

-forcing reactions from those affected, justifying terrorist actions;

-destruction of targets and producing considerable human and material damage;

-the psychological influence of some decision structures and the corruption of public opinion.

Unprecedented increase in available resources to terrorist organizations, almost unlimited access to the technological, bio-engineering and applied chemistry information hold key positions, offering the possibility to improve the system of management and execution of attacks, while diversifying the means used to achieve objectives.

The asymmetrical way of action of terrorist organizations over the civilized world, failure of law rules or norms of armed conflict, international law or at least ethical rules dictated by the assumption of general human values accepted by the civilized world reduces the predictability of their actions and therefore increases the hazard of terrorist actions, increasing their effectiveness.

2. LATEST SCIENCE AND TECHNOLOGY ACHIEVEMENTS IN PREVENTING TERRORIST ACTS

The international dimension of counter-terrorism policy has become of great importance both in terms of cooperative political support efforts and, above all, the harmonization and joint efforts of all elements responsible for combating terrorism. In this context, we are witnessing an impressive group force capabilitie, backed by political consensus, unimaginable some time ago.

Armies, no matter how prepared, can not manage with the means they have to carry virtually the fight against international terrorism. Apart from special forces and informational sensors, they have structures capable to act symmetrically against networks and terrorist groups. It remains to be seen whether, in the future, they will create such structures involved in fighting terrorism, or will act according to their specificity, because it is unlikely that states will waive the armies and structured for a war against armys and create armed military forces modeled exclusively for the war against terrorism.

However, it is possible to broaden the special forces army structures able to act against all types of terrorism, in close collaboration with other forces and intelligence services in particular. We believe that the tasks that the armies (with the current structure) can preform generally in the following area:

-detection by informational sensors and special forces training centers regarding international terrorist organizations and networks ;

-hitting, by military means, especially aviation, missiles of all types and special forces, vital centers, training bases, warehouses and terrorist infrastructure in home zones (as they are discovered and identified and obtained approval of the country or countries in which they are located), most often in cooperation with the armed forces of these countries and/or other forces in the area;

-the war against terrorism (armed struggle) by the anti-terrorist coalition, with or without UN mandate, against countries and political regimes that practice or harbor terrorist groups and support/fund the terrorist or criminal actions;

-participation in search and destroy missions of bases and terrorist networks in fault zones;

-participation in conducting special operations against international terrorism. (Mureşan, M., Văduva,G., 2004: 471 – 474)

The performance of these tasks involve, of course, action force, aimed at destroying targets, force structures and technical elements of networks and terrorist organizations. Therefore, they are action over effects. They must act on causes. A substantial contemporary method of combating terrorism, which gives, in essence, as a fault terrorism, can not be achieved only through a series of anti-fault programs and strategies, long-term and very complex. These programs should aim, in particular the following:

-reducing the technology gap between the participating countries and harmonization of their interests;

-reactivation / awareness of international democratic organizations ;

-waiver of influence policy, irreconcilable and pressure power centers ;

-promoting sustainable procedures for the crisis management and conflict ;

-creation of flexible structures to detect networks and terrorist organizations and to address them through appropriate means (which is not in the power of armies structured prepared to take arms, nor wars with other governments that have clear strategies against non- actors);

-social harmonization, involving all countries, international bodies and organizations, wherever terrorist threats may come from; the need for a global response.

In the contemporary operational environment, the effective management of terrorist crisis use new science and technology achievements in both preventive and combatant actions. Thus, in recent years, one of the technological options in the fight against terrorism is represented by the biometric branch of science that deals with the measurement of the biological characteristics of a person. This category includes fingerprints, hand geometry, iris scanning and facial recognition. Since biometric parameters can not be lost, forgotten or transferred from one person to another, they are already widely used as specific security measures.

Biometric systems aimed at two main goals. One is identification (who is the person?) by which the identity of a subject is determined by comparing a biometric parameter measured with existing databases. The second is to check (is this person who he claims to be?) within which a biometric parameter measured is compared with that of a particular person. All biometric parameters can be used for verification, but only the unique (especially fingerprints, iris scans and facial recognition) can be used for identification. Biometric parameters are mainly used for access control, to ensure that a particular building or premises shall only be accessed by a authorized persons.

Hand geometry-based systems are ment to measure the shape, size and other characteristics of palms witch are used to control access and check the identity of people in airports, offices, factories, schools, hospitals, government institutions etc. Since hand geometry is a technique of verification, not of identification, users are asked to indicate who they are (inserting a card before scanning). Biometric parameters are then compared with those of the persons.

Extending access control technology is now fully justified. In the security tests achieved in 2001 by America's Federal Aviation Authority, attempts to enter the security zones have been successful in 31% of cases, and the inspectors were able to verify ("boarded") about 80 aircraft.

Another biometric technique witch began to be used successfully in airports is iris scanning. This has already yielded good results in dozens of U.S. prisons to identify inmates, staff and visitors. Also iris scans have been tested by banks to identify the users of ATMs. With their aid, customers do not have to introduce a note card or personal identification number.

Face recognition is the only biometric technique that can be used passively, by comparing the image of a figure with a database of suspects. Such systems connected to a network of closed-circuit television, are already used in the UK stadiums to identify the famous "hooligans".

The director of American companie specialized in this field said that the verification of fingerprints and iris scan would not have paid off with the hijackers of 11 September 2001, but facial recognition would have been effective. "What you need to do is to constitute a database of international terrorism, with photographs and fingerprints of all persons suspected of such acts." Then all passengers would be required at the time of entry into the airport, to undergo a facial scan, "just like your credit card is verified when you buy something with a credit card." Many of the air pirates are not known members of a terrorist organizations, and therefore their data does not appear in such databases.

Another technology that enjoys growing interest is the three-dimensional scanners or scanners "threat image projection" (threat image projection - TIP). The TIP scanner principle is to project the image of a randomly threat on the luggage (knife, gun, bomb component). When the scanner identifies a similar object, illuminates a warning light and the luggage can be retained for a thorough check. The terrorists of September 11, 2001 used as weapons objects that such scanners would not report them as threats.

In the face of terrorists who do not carry weapons and who are traveling under their own identity, a new efficient technology could be computer-assisted verification of passengers (computer - assisted Passengers screning) experimented in 1998 by some U.S. airlines.

It uses information from the system reservation program and the history of previous trips by a person to identify potential suspects to be subjected to additional security procedures.

If identifying the terrorists at ground level is so difficult, what might be done for planes to be harder to hijack in the air? Former president of the British Airlines, Robert Ayling, suggested that the passenger planes could be fitted with a system for controlling them from the ground in case the plane is hijacked. Such a system of remote distance control can be penetrated and used by hackers employed by terrorists. Another suggestion is to modify the existing automatic collision avoiding system so that an deliberately impact can be prevented.

3. CONCLUSIONS

In the days following the attacks of 11 September 2001 politicians and the authorities have realized how little they know about the promoters of the attack and their motivations. Books on the subject were present, most been available in bookstores or on the Internet. The war in Afghanistan, U.S. support for the mujahideen and the Taliban regime are detailed in the works Taliban (MJ Gohar, Oxford University Press) and Unholy Wars (John Cooley, Pluto Press, London). The second, written by an American television reporter accuses U.S. of the results of what some call the CIA Jihad in the 80s. However, no matter how advanced the technology used might be, it should be handled by trained personnel, the human factor being impossible to control. The reality is that the terrorist threat can not be removed with the help of technology.

REFERENCES

1.Antipa Maricel, (2004). *Securitatea şi terorismul. Prevenirea şi combaterea acţiunilor extremist-teroriste pe teritoriul României. Tendinţe şi perspective la început de mileniu*, Editura Celsius, Bucureşti.

2.Frunzeti Teodor, Zodian Vladimir, (2011). *Lumea 2011. Enciclopedie politică şi militară*, Editura CTEA, Bucureşti.

3.Frunzeti Teodor, Zodian Vladimir, (2013). *Lumea 2013. Enciclopedie politică şi militară*, Editura RAO, Bucureşti.

4.Mureşan Mircea, Toma Gheorghe, (2003). *Provocările începutului de mileniu*, Editura U.N.Ap., Bucureşti.

5.Mureşan Mircea, Văduva Gheorghe, (2004). *Războiul viitorului, viitorul războiului*, Editura Universității Naționale de Apărare, Bucureşti.

6.Păun Vasile, Popa A., (2002). *O provocare strategică: Războiul informațional*, Bucureşti Editura U.T.I.

7.Primakov E., (2003). *Lumea după 11 septembrie,* Editura Institutului Cultural Român, Bucureşti.

8.Randall M., *Le terrorisme de demain risque d'être nucleare, dit Bush a l'ONU,* www.fr.news.yahoo.com

9.Simileanu Vasile, (2003). *Asimetria fenomenului terorist*, Bucureşti, Editura Top Forum.