CBRN TERRORISM: A CONTRIBUTION TO THE ANALYSIS OF RISKS

Dušan VIČAR*, Radim VIČAR**

*Tomas Bata University, Department of Crisis Management and Logistics, Crisis Management Institute, Uherské Hradiště, Czech Republic
** University of Defence, Faculty of Economics and Management, Brno, Czech Republic

The World Trade Centre attack of September 2001 and the subsequent anthrax letters brought the need for Chemical, Biological, Radiological and Nuclear (CBRN) counter-terrorism preparadness into focus. By and large, our understanding of the nature of CBRN terrorism derives entirely from military the paradigm of chemical and biological warfare. An examination of recent CBRN terrorism events such as the 1995 Sarin attack on the Tokyo subway system by a terrorist cult and the 2001 anthrax letter attacks in the United States of America show that the military paradigm of CBW defence cannot be applied to CBRN terrorism.

Key words: *Chemical, Biological, Radiological and Nuclear Terrorism, CBRN agents, CBRN terrorism, CBRN Counter-Terrorism.*

1. INTRODUCTION

Terrorism is a socially dangerous phenomenon both at the national and international level. It is a deliberate, preconceived use of force or threat of force, usually often focused on not involved persons to trigger a fear, through which terrorists' political, ideological and religious requirements are to be met. In a global war, everyone is a target of terrorists, especially unprotected civilians, as they are the easiest target. Definitions of terrorism have certain common elements emphasizing the systematic use of physical violence directed against civilians to cause a general climate of fear when innocent people are targeted for political and social change. There are no commonly accepted definitions of CBRN materials, threats or incidents. For the purpose of this paper, however, it is most useful to use a rather broad description of the terrorist threat concerning CBRN materials: all uses of chemical, biological, radiological or nuclear substances and materials for terrorist purposes.

An increasing interest of terrorists in chemical and biological warfare agents, an easy access to technical information, technologies, materials and specialist data and an increase of terrorist attacks with the use of chemical and biological weapons highlight the fact that the risk of this kind of terrorism is

growing. Chemical and biological agents attract terrorists because their production is easy and can be easily acquired. Even a small amount of these agents, due to their toxicity and contagiousness, can result in heavy losses of unprotected population. Of course, terrorism does not use only such chemical and biological agents, which are designed for special military purposes. Just realize a great amount of tanks transporting industrial toxic agents on roads and by railway, which may easily become a focus of terrorist action.

An exact number of casualties or losses of lives because of CBRN assets usage cannot be estimated, but experts agree that the greatest effect of their use will be a large-scale wave of fear and panic. Awareness of public and readiness of special units of the so-called first responders (*i.e.* fire-fighters, police personnel, emergency medical and rescue service) to a CBRN terrorist attack can prevent an uncontrolled spreading of fear and panic and, consequently, will impede terrorists to attain their main objective- to scare and dismay their victims.

2. HISTORICAL EXAMPLES OF THE USE OF CBRN DEVICES IN TERRORIST ATTACKS

On 20 March 1995 in Tokyo subway, a sarin, chemical agent, was used for a terrorist attack against non-protected civilians. A religious cult Aum Shinrikyo acquired information and technical means to plan, produce and use chemical agents for its own terrorist goal. This attack was a first example of a large-scale terrorist attack with the use of toxic chemical agents that was considered by that time to be a domain of military forces.

The impact of this terrorist attack was measured in terms of numbers of casualties and injured, gaps in the technical capabilities of first responders and a clear demonstration of the use of CBRN assets to attain the targets of terrorists. The sarin attack affected 5,100 persons, out of which 12 were casualties, 40 heavily affected, more than 900 moderately affected and many slightly injured. About 300 members of the rescue teams, including fire fighters, policemen and emergency medical personnel were also injured. These secondary victims were caused by insufficient knowledge, training and technical capabilities to cope with a threat posed by the use of chemical weapons. It also revealed the fact that those who want to rescue must be properly protected.

This sarin attack also showed how important were the means to handle with immediate consequences of threat, such as, for example, protective equipment for rescue teams, detection and diagnosis equipment, means for hasty decontamination of victims, rescue teams and buildings, and how important a proper coordination and communication of individual

first responders against this type of terrorist attack was.

In October 2001 in the U.S. a series of anthrax attacks occurred. The first information of affected persons came from Florida. Other cases of anthrax inhalation and skin infection appeared in New York, New Jersey, Maryland, Virginia, Pennsylvania and Connecticut. Letters containing powder anthrax were sent to various mass media and state administration authorities. In total, there were 22 affected persons, 11 of them with symptoms on their skin and 11 more with respiratory system problems. Due to the inhalation of the agent, 5 people died.

This case shows another example of the use of CBRN assets for terrorist attacks. Same as in Tokyo, terrorists acquired necessary information and equipment needed to launch an attack using the biological warfare agent. The so-called anthrax letters showed that use of combat biological agents could have new intended or not intended aftermaths that were not sufficiently evident in connection with the use of chemical and biological agents to date. The impact on the civilians was terrible (32,000 persons had to undergo a basic antimicrobiological treatment, out of them more than 10,000 persons due to a suspicion of being contaminated by this anthrax were recommended to undergo another 60-days treatment). Another effect of anthrax letters was a great contamination of buildings and infrastructure. Some post office personnel were contaminated and several died. If we take into consideration a characteristic of the terrorist attack already mentioned in the second example (*i.e.* the letters were carefully stuck down and an explanatory message was attached) it is improbable that the post office personnel were also an objective of terrorists. The consequences of these anthrax attacks were solved months and years after this event, as opposed to an immediate emergency in case of attack by chemical warfare agent.

These attacks showed a need to quickly detect the attack, identify its character and, given the nature of the attack, to also diagnose the persons contaminated by anthrax, which posed an enormous burden on the health care system. It was also necessary to find the contaminated persons and to provide them a timely and proper care. While great efforts were made to remove the attack consequences, the specialized laboratories processed more than 120,000 tests for B. anthracis, 69% of which were carried out by the laboratories of the public medical facilities. For preventive and curative care, 3.75 million antidotes were needed. This called attention to the need to improve readiness and immediate response, which had not been so urgent in the case of previous terrorist attacks.

3. CBRN TERRORISM ATTACKS EXPERIENCE

With the attack against the World Business Center in September 2001 and following letters containing anthrax, security and the need to be prepared to counter chemical, biological, nuclear and radiological

attack became the focus of attention of strategic planning and national security of almost all countries. Since then they have been considered as one of the most important challenges to the democratic civilization. From a general viewpoint, a present understanding of the substance of terrorism that uses chemical, biological, nuclear and radiological assets issues especially from a military paradigm of the conduct of chemical and biological warfare. These paradigms include tasks of intelligence service, lists of potential threatening by CBRN assets, assessment of potential targets of attack, risk analysis and conception of defense as a deterrent means. However, from an analysis of terrorist attacks with the use of CBRN assets it results that against terrorism, which uses the CBRN assets, a conception of defense against chemical and biological warfare in an armed conflict cannot be applied.

To attain a better readiness for defense against terrorist CBRN attacks, as well as development of prevention and response methods, it is necessary to create new models of better response to such attacks. A present approach to countering this type of terrorism resembles the approach to a military threat, namely the use of the intelligence service to identify the capabilities of an enemy, to have proper knowledge of NBC weapons threat designed by an enemy for combat purposes, analysis of related risks and weapons that can be applied, and also the assumption that a well prepared defense will discourage an enemy from an attack. The question is if these assumptions are valid.

Terrorism, especially CBRN terrorism, calls for new approaches to intelligence information. It requires collecting, analyzing and exchanging information not only on the organizations, but also on the individuals that work independently. There are very little events reviewed in such a great detail as the attacks of 11 September 2001 in New York and Washington and attacks by anthrax-laden letter. The intelligence services, especially, were criticized because they did not provide timely warning so that preventive action could be taken. Taking into account many indications that terrorists hired new members, trained them, planned and organized attacks, as well as the duration of the preparations to counter these, as mentioned by the media, the activity of the intelligence services can be perceived as a failure. However, it is necessary to admit that from the actions of individuals who pursue wider terrorist goals, it is not simple to acquire "*information*" needed for an effective countering of a terrorist attack.

The military science, due to the transition from conventional weapons to the new non-conventional conduct of combat, started to use the term of "*asymmetric war*". Terrorism is sometimes considered a civilian analogy to asymmetric war, where small-scale non-conventional attacks have a great impact. On the other

hand, other sources view this analogy as imprecise because the target of the attack is not the armed forces, but unprotected civilians.

4. LEGAL INSTRUMENTS AND CBRN TERRORISM

Terrorist attacks have highlighted the need for further efforts of the entire international community in combating this threat. In the fight against global terrorist networks national or regional response is insufficient. Global cooperation thus becomes a matter of vital importance. For example, the European Union is a key player alongside with the United States of America (USA), China and Russia, on the international scene and has a decisive influence on the security situation in the world. By its nature, it is a supranational organization, the body of international relations that, after the adoption of the Lisbon Treaty, has a legal personality. The threat of a terrorist group acquiring CBRN materials has led governments and international organisations to adopt far-reaching regulations and programmes to defend populations against the associated risks.

A common European approach to security issues of the contemporary world was outlined in December 2003 when the EU Council met in Brussels and adopted the final version of the European Security Strategy (ESS). For the first time principles were established and clear objectives for the enforcement of security interests of the EU based on core values and identified a range of threats and challenges to security concerns set. The main threats classified in the ESS are: terrorism, proliferation of weapons of mass destruction, regional conflicts, state failure and organized crime.

These threats were described as new, more diverse, less visible and less predictable. On the other hand, the traditional military threat in the form of large-scale aggression against any Member State of the EU seems unlikely. The ESS considers an attack using CBRN weapons as one of the biggest threats to the security of the EU, especially thanks to advances in biological sciences which may increase the potency of biological weapons. The most frightening scenario is terrorist groups gaining CBRN weapons. In such a scenario a small group could cause damage similar to what was previously possible only for states and armed forces.

Tackling terrorist access to CBRN material is currently considered a priority for the European Union. This is acknowledged by the European Union Counter-Terrorism Strategy adopted by the Council on 1 December 2005, and by the *"EU Strategy against proliferation of weapons of mass destruction and their means of delivery (WMD)"* adopted by the European Council on 12 December 2003.

The EU counter-terrorism strategy fights against terrorism on four main objectives: prevent, protect, pursue

and respond and with wide range of measures (co-operation in fields ranging from intelligence sharing to law enforcement and the control of financial assets in order to make it easier to find, detain and bring to justice terror suspects).

The overall goal of CBRN policy is to reduce the threat and damage from CBRN incidents to the citizens of the European Union, by way of a coherent, prioritised EU CBRN Action Plan. The EU CBRN Action Plan is not a legal instrument. The Action Plan foresees three main areas of CBRN security work: Prevention (*i.e.* ensuring that unauthorised access to CBRN materials of concern is as difficult as possible); Detection (having the capability to detect CBRN materials in order to prevent or respond to CBRN incidents); Preparedness and response (*i.e.* being able to efficiently respond to incidents involving CBRN materials and recover from them as quickly as possible).

Protecting the population from terrorism and other criminal threats is a high priority for the EU. As exemplified by events around the world, there is continuous interest of terrorists in acquiring CBRN materials. The Member States are primarily responsible for many of the areas of work which are covered by the current policy package. They are responsible for protecting their citizens from CBRN threats by a host of different measures, and with the involvement of a wide range of responsible authorities.

5. A DEFENCE AGAINST CBRN TERRORISM

In defence against chemical and biological agents and in technical preparations, agents known to have been developed and used by an enemy as a weapon have always been highlighted. Such agents are on the list that serves as a basis for the development of protective technical means and capabilities, including presence detection, identification, protection, medical measures and elimination of effects of these agents. The above-mentioned emphasis on known chemical and biological warfare agents, even bias towards these agents, led the military to conceived the defence against such an attack as a defence against a "specific threat". Thus, defence against terrorism, in a way, can be viewed as defence against a "non specific threat". A spectrum of CBRN means of attack provides terrorists with a nearly unlimited amount of toxic, hazardous and infectious agents, the production, stocktaking, tactical or strategic use of which are not included by military into a traditional analysis of risks. That is why, in coping with terrorist attack, civilian first responders must apply an integrating approach, which takes into an account all types of threat.

Based on the intelligence information and analysis of threats and risks, in order to minimize impacts of CBRN attack, militaries must invest into the defense and protective equipment. They perform training to ensure a minimum impact

on the armed force's operational capabilities in case of eventual CBRN attack. Also, a proper assessment of the technologies and the new possibilities to support chemical and biological defense on the basis of prediction of potential threat in the next 10-15 years is used. The result of this assessment is identification of areas where knowledge should be amended, as well as recommendations on how to achieve it submitted. A part of this assessment is also a presumption that these technologies, if used, will serve as a deterrent. Certainly, this consideration assumes that enemy's behavior is rational or that enemy is able to analyze strategic or tactic employment of chemical weapons and take decisions based on the level of defense and capabilities of the opponent.

However, this assumption does not apply to terrorism. Traditional deterrent means that it cannot stop a group of dissenters without any concrete objective. Terrorism that uses the CBRN assets has the greatest deterrent and destructive effect because its target is unprotected civilian inhabitants. There are not such measures that could protect civilian inhabitants under all circumstances. Even the strictest security and preventive countermeasures cannot prevent suicide assassins. There will always be vulnerable groups of people. A targeted protection, for example, of significant buildings, cities or various events can make terrorists change their plans and attack other, less protected groups of people.

A critical issue is the training of the first reaction forces for CBRN attack. Before the personnel in the first line can say what action must be taken and what equipment they need to eliminate the aftermaths of such attack, they must understand the basic aspects of chemical, biological and radiological agents. Though an average rescuer does not need to be a chemistry expert for these agents, nor must he know how to treat every approximately 300 human pathogens, he must anyway know symptoms of effects of these agents and basic treatment and decontamination procedures. Having this information, he is able to transform his knowledge and experience and apply them in a case of terrorist attack.

In the case of threat from potential hazardous agents the rescue technical teams use standard procedures which encompass basic target functions like site inspection for threats, hazardous agent identification, risk and threat analysis, assessment of protective equipment necessity, information and rescue resources co-ordination, hazardous agent control by preventing its spreading, decontaminating the area and consolidating the overall situation. After a terrorist attack, other important functions must be added: people's evacuation, casualties' clearance and treatment and evidence material gathering.

6. CONCLUSIONS

The CBRN terrorism counter-measures, in contrast to the recommendation of the armed forces structures, require shifting from a

decision-taking process based on the detailed analysis of the enemy capabilities to an approach based on the risk analysis. To establish priorities, many countries carried out extensive consultations resulting in risk analyses of the CBRN assets. Conclusions of such analyses are used by intelligence services, anti-terrorist units, scientific agencies and institutions and rescue teams that have to cope with actual events.

However, a detailed research of the potential use of CBRN assets for terrorism does not guarantee that an actual CBRN attack can be avoided. Risks related to the use of CBRN assets and materials show how important it is to have consolidated capabilities available to respond to the threat and properly train rescue teams for a partnership within a scientific-technological community. Knowledge on CBRN assets that ensue from the usual military practice of preparedness must be carefully reviewed and immediately quit if they do not meet the for civilian protection requirements in case of threat. It seems to be vitally important for the EU Member States to ensure: legislation (which determines the duties and responsibilities of citizens in the constitution and other laws in accordance with EU strategic and legal principles), the systematic training of experts in the field of crisis management, performance and intelligence cooperation at bilateral and multilateral international levels, scientific research and technological cooperation, the systematic preparation of specialists (special forces) to combat terrorism, population information and preparation, a functional integrated rescue system, finance and logistics.

REFERENCES

[1] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union.

[2] Countering Terrorism. Final Report - Part I (2003), RTO/SAS-049 Specialist Team. Brussels.

[3] Evropská bezpečnostní strategie [online]. Council of the EU, [cit. 2011-5-10]. http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.

[4] Jenkins, Brian. *International Terrorism: The Other World War.* In Charles W. Kegley, Jr. (ed.), (2003) The New Global Terrorism: Characteristics, Causes, and Controls. Upper Saddle River, NJ: Prentice Hall, ISBN 978-0130494139.

[5] Kournikakis, B., et al., (2001) *Risk Assessment of Anthrax Threat Letters.* DRES Technical Report 2001-048, Defence R&D Canada.

[6] Laqueur, Walter. Postmodern Terrorism. In Kegley, Jr. (ed.), (2003) The New Global Terrorism: Characteristics, Causes, and Controls. Prentice Hall, NJ Upper Saddle River, ISBN 978-0130494139.

[7] Proceedings of Lecture Series on Chemical and Biological Defence (2005), Brusel, RTO NATO.

[8] *RTO Combating Terrorism.* Workshop Report. USA, Arlington, 2002.

[9] Svoboda, I., *et al.*, (2010) Politický extremismus a terorismus jako ohrožení vnitřní bezpečnosti státu. Univerzita obrany, Brno, p.144, ISBN 80-7418-046-0.