http://dx.doi.org/10.18778/8142-184-3.01

Mariusz Grasza and Marcin Podogrocki

INTRODUCTION

Contemporary world evolves on many planes, including terrorist threats. Who is a criminal armed with conventional weapons, explosives, attempting to provoke fear, panic and paralysis to manifest their views or achieve other benefits? It is a simplified and common perception of a terrorist seen through the eyes of the shortest century – the 20 century. History of civilisations knows some cases of attempted unconventional warfare, even by using pathogens, as evidenced by the examples listed below:

– 1346 (Theodosia) – the Tatars hurled plague cadavers into the city of Caffa during a siege.

– 15 and 16 century – the conquest of America - Pizarro gives a smallpox-infested gift to the natives.

– 1710 – during the war with Sweden in Peter the First times, Russians hurled plague cadavers into the city of Reval.

– 1767 – a smallpox virus-infested blanket distributed as a gift by the British general, Jeffrey Amherst, to the Native Americans.

– 1797 – an attempt to spread a swamp fever pathogen during Napoleon's warfare operations at Manuta.

A long list of historical events which involved using naturally occurring potential threats to human organism could be given her. They were made in order to direct their negative impact to the adversary.

The CBRN potential has been and is appreciated by distinguished strategists, which translated into development and classification of a new warfield weapons, namely the Weapons of Mass Destruction (WMD). Used mostly for military purposes, WMD has become well sought-after by terrorist groups. In the era of the so-called "super-terrorism" threats, CBRN is perceived as an asymmetric struggle which does not apply to armed conflicts and is oriented towards destabilising the internal state security system.

The process of preparing for a terrorist attack has gained a new dimension. Apart from the attempt of an illegal acquisition, seizure of hazardous chemical, biological, radiation and nuclear (CBRN) agents, criminal groups put an emphasis on the acquisition of technology, technical knowledge or individuals who make own production of "the CBRN threats" possible.

CBRN refers to hazardous chemical, biological, radiation or nuclear material. While some materials classified to CBRN are used daily for the good of humanity,

its improper use may create hazard for all forms of life and environment, in which we live. On the other hand, a potential size of consequences may be dependent on many parameters (a type of an agent, its quantity, its dispersion method, attack site/place, weather conditions, etc.).

CBRN education was initiated in response to the need to strengthen the internal security potential of the EU states to counteract potential threats that come with use of a hazardous chemical, biological, radiation or nuclear agent for terrorist purposes. A terrorist attack in Tokyo metro may come as an excellent illustration of the need to educate in the CBRN area. On 20 March 1995, Aum Shinrikyō religious sect sprayed a poisonous warfare agent, sarin, in a metro train at Kasumigaseki station. The CBRN terrorist attack caused 12 deaths and affected more than 5 thousand victims, who were injured. The services were not appropriately prepared, lacked knowledge and equipment and, in consequence, the responding rescue services were exposed to a poisonous warfare agent. As a result, 135 members of rescue teams involved in the response operation suffered. Also note that, long after the attack, many persons suffered from illnesses resulting from remaining in sarin-contaminated zone, including depression, breathing difficulties or brain damage.

It is possible that CBRN factors will be used in the aspect of transformation of states, geopolitical conflicts, and religious conflicts as spectacular terrorist attack. Crime may be caused political, religious, economic or national motives. Potential culprits likely to be placed at the heart of a terrorist attack include:

– governmental buildings and complexes;
– politicians;
– public utility buildings;
– critical infrastructure;
– the infrastructure used to transmit chemical compounds classified to CBRN factors;
– complexes/buildings where agents potentially useful for a CBRN attack are manufactured or stored;
– objects of religious cult;
– means of mass transportation;
– (road, rail and water) transports with agents which can be potentially used for a CBRN attack;
– large population concentrations.

One may assume that terrorists will stress the largest possible dispersion of the hazardous CBRN agent, with the use of:

– explosives;
– technical measures such as compressed aerosols, unmanned aircrafts;
– contaminated live organisms.

Potential consequences of a terrorist attack may include:

– human casualties (fatalities, injured, wounded, ill);
– losses in the critical infrastructure;

– interruptions in access to core municipal/communal services such as: environmental pollution, medical/health care, power supply, water supply, ITC, public transport;

– economic losses (costs of decontamination, rebuilding, commercial/trade losses, high costs of treating the ill);

– political consequences (undermining stability of the state security).

In terms of scale, a CBRN incident may be vast and trans-border and, as such, it may require international reaction. In order to understand the essence of the CBRN issue, one must understand their impact on human life, health and the environment.

The first threat described in the CBRN acronym is "C" which refers to chemical compound – they may be used in terrorist attacks due to their toxicity i.e. their chemical properties may cause death, permanent damage to one's health or temporary incapacity for work. They are divided into chemical warfare agents (CWA) mostly used for the military purposes) and toxic industrial agents (TIA, used mainly in enterprises, households, public and private institutions which ensure satisfaction of community needs). Chemical warfare agents are the basic component of chemical weapons, responsible for the mass nature of paralysis. They are classified on the basis of poisoning symptoms and the goal to be reached.

CWA classification based on the symptom-related criteria:

– nerve agents;
– blister agents;
– pulmonary agents;
– blood agents;
– psychotic agents;
– irritating agents.

In the tactical application context, the CWA may be divided into:

– lethal warfare agents;
– paralysing warfare agents;
– exercise warfare agents.

Due to high toxicity and long field life, nerve agents are predominantly used in the form of organophosphorous compound such as sarin, soman, VX and blister agents such as sulphur mustard (mustard gas) or lewisite.

The scale and impact of using such poisonous warfare agents during WWI, Iraqi-Iranian war or quite recently (on 4 April 2017) in Chan Schaychun in Syria, chemical weapons may be also used in terrorist attack and Tokyo metro terrorist attack is a good example of such use. However, the majority of the states decided to fully eliminate a potential use of chemical weapons by introducing provisions of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction of 13 January 1993.

CWA's may be also used in terrorist attack and Tokyo metro terrorist attack is a good example of such use. CWA chemical compounds are illegally produced

for such purposes and, in spite of legal restrictions and intensified control; the EU states cannot fully guarantee that they are not acquired by potential terrorists. A potential attempt to smuggle precursor for synthesising CWA into a country which is a potential target of a terrorist CWA attack initiates prevention and deterrence measures in countries. They involve launching a process of modernising the technical equipment used for monitoring and detecting hazardous chemical compounds on border points. The Border Guard is responsible for preventing any illicit traffic of any psychotropic agents, weapons, munitions, explosives, radiation material and hazardous chemical substances across the state border. Anti-terrorist measures taken by states involve not allowing any persons suspected of any terrorist activity into their territory as well as preventing such persons from exiting the country. In Schengen zone, prevention measures are largely based on international collaboration also in the area of exchange of information and joint operations as well as on ensuring tightness of external borders by each Schengen state. The above arises from the system of borders open to all EU members Such a significant protection-related challenge is also exponentiated by free movement of persons inside Schengen zone, which does not only apply to the states – signatories but also to any nationalities and any citizenship who cross internal borders within the area to which Schengen treaty applies.

A threat of smuggling CWA may arise from the geopolitical situation but also from engagement of some terrorist organisation in an attempt to manufacture such weapons. It is likely that the so-called Islamic States has the technology, know-how and access to the materials which can be used to produce the CWA.

It is easier to initiate a terrorist attack with a use of Toxic Industrial Agents and, while such attack may seem less spectacular, its consequences for human life, health, the environment and the economy are serious.

Such threat may be come from a wilfully caused failure or a catastrophe in industrial complexes (which manufacture or process chemicals). Each industrialised country has many complexes of such kind.

One should be aware that it is possible to cause a transportation (rail, road, sea or air) catastrophe in which terrorist will be interested in unsealing transported toxic industrial agents. The pipeline infrastructure used for transporting TIA may be also the target of attacks classified as CBRN.

To comprehend the scale of the TIA threat it terms of their area coverage, according to the EMERGENCY RESPONSE GUIDEBOOK-2016 issued by the US Department of Transportation, in case of a large leak of chlorine one should assume that contamination will spread within the radius of 275 m from the epicentre of the agent release and the range of the warning zone in the wind direction should be 2.7 km during the day and 6.8 km at night, respectively. For this reason, the issue of a TIA or CWA threat to the population as a result of a terrorist attack applies not only to the epicentre, the potential contamination area (e.g. the site where the railway infrastructure or a power plant is located)

as well as the alarm area i.e. an adjacent area whose population is exposed to the potential risk of the toxic agent.

The second threat included in the CBRN acronym is "B" which applies to potentially hazardous pathogens e.g. micro-organisms, bacteria, fungi, toxins produced by micro-organisms or plants and newly appearing pathogens which may be created through genetic engineering manipulation to enhance their spreading.

The US federal government agency which operating under the Department of Health and Human Services – CDC (Centres for Disease Control and Prevention) introduced 3 categories of the hazardous biological agents:

– Category A – pathogens which are easy to disseminate and therefore result in high mortality rates e.g. anthrax, botulism, and tularaemia.

– Category B – pathogens which are moderately and easy to disseminate, of moderate morbidity and mortality, e.g. Bang's disease, Melioidosis (*Burkholderia pseudomallei*), Q fever, Glanders (*Burkholderia mallei*).

– Category C – pathogens which are easily accessible and easy to disseminate and, therefore, may cause high morbidity and mortality rate e.g. newly emerging pathogens which may be subject to genetic engineering manipulation for the purpose of more effective dissemination.

Some of potentially hazardous pathogens which may be used in bioterrorist attacks:

– Gram-positive *Bacillus anthracis*;
– Gram-negative *Yersinia pestis*;
– *Vibrio cholera*;
– Gram-negative *Francisella tularensis*;
– Gram-negative *Burkholderia pseudomallei*;
– Gram-negative *Coxiella burnetti bacteria*;
– Gram-negative *Brucella pestis*;
– Gram-negative *Chlamydophila pneumonia*;
– Gram-negative *Neisseria meningitides*;
– Drug-resistant gram-positive *Streptococcus pneumoniae* and *Staphylococcus aureus* bacteria strains;
– Poxvirus variolae smallpox Virus;
– Bunyaviridae family Virus;
– Junin Virus;
– Machupo Virus;
– Marburg Virus;
– Ebola Virus;
– Eastern equine encephalitis Virus;
– Lassa Virus.

Pathogens were used for terrorist purposes for example in the case of salmonella-poisoning salad bars in the Dallas, Oregon, USA, in 1984 by Rajneeshee Cult organisation, resulting in mass poisoning of 751 people. The purpose of the attack

i.e. preventing the local community from voting in the elections, was disclosed one year after the incident. Other examples could the terrorist attacks with the anthrax-contaminated correspondents on the territory of the USA. They began on 18 September 2001 and lasted for several weeks. Letters containing anthrax spores were posted to several offices of news agencies and to two Democratic senators. They resulted in 5 fatalities and approximately 17 persons becoming ill.

How serious may a terrorist attack with a pathogen be? It took more than 2 years to decontaminate Brentwook post site while the Hamilton post in New York was closed until March 2005. Unofficially, all losses in fixed assets caused by the CBRN terrorist attack are estimated at 1 billion USD or more.

Note that states do notice a potential threat represented by the biological weapons e.g. because of more difficult control. On 10 April 1972, in London, Moscow and Washington the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Biological Weapons Convention, BWC) was signed. At present, 178 states are bound by the BWC.

The next type of hazard represented in the CBRN acronym is the RN which refers to a terrorist attack involving radioactive isotopes. WMD nuclear threats may be analysed as special nuclear material and other substances capable of nuclear reaction as well as other radioactive isotopes which may be used in a device designated for dispersion of radioactive contamination. The importance of the issue is illustrated by the Activity of nuclear material intercepted by law and order agencies, which can be potentially used for production of the weapons, in the past 10 to 15 years. According to the International Atomic Energy Agency, since 1993, more than 300 bans on radioactive substance trading have been introduced, including 17 bans on special nuclear material. Special nuclear material is a category of radioactive substances used for production of nuclear weapons, including plutonium, enriched uranium 235 and uranium 233. Huge efforts are taken to ensure the proper control of their transport and storage. In spite of that, cases of intercepting illegally traded nuclear material have been reported. More than 15 kg of highly enriched uranium and 400 g of plutonium was confiscated. Europol estimates that currently, additional 10 to 30 kg of enriched uranium is now being traded on the black market.

Other radioactive isotopes which could be used in the form of dispersion contain some nuclear material but it does not apply to fissionable reactions. Dispersion devices may be built from conventional explosives and a radioactive isotope and their purpose is to disperse radioactive substance causing contamination of the population and its environment. These may be radioactive substances used in medicine and in the industry, orphaned, abandoned or illegally acquired. Hazard in such form may lead to disruption of the public order. Such actions generate enormous costs of decontamination and social panic. The society is governed by stereotypical image of radiation causing fear and a mental block.

After a terrorist incident involving RN, the local community may disapprove using decontaminated sites/ location in spite their successful decontamination. There are millions of radiation sources used on our globe. Many of these sources are weak which translates into an insignificant threat. The International Atomic Energy Agency has a global list of more than 20,000 entities which hold or own radioactive sources i.e.:

– more than 10,000 sources used in medicine;
– more than 12,000 sources used in the industry.

Note that there are countries and regions which leave a lot to be desired for when it comes to the rules for keeping inventory of their radioactive materials. The above-presented numbers illustrate the scale at which radioactive isotopes are used and the potential risk of their sealing or interception for terrorist purposes consequent upon the number. There are several reasons for stealing radioactive isotopes:

– radioactive isotopes stolen for the purpose of illicit trading (for profit);
– theft of some assets (a car, material bringing a high price when sold as scrap metal) containing a radioactive isotope (the perpetrator unaware of a radioactive isotope existing in the stolen goods);
– radioactive isotope stolen to be used for terrorist attacks.

Customs officers, border guard officers and the police reveal many attempts at smuggling and selling stolen sources. State security may be undermined by the radioactive sources which:

– has never been recorded and are unaccounted for (lack of relevant legal regulations in the country or non-compliance);
– had been controlled but their chain of custody was broken due to lack of appropriate supervision (have been abandoned, lost or disappeared);
– have been stolen or removed without an appropriate permit.

For the above-given reasons, the number of orphaned sources globally remains unknown but it is estimated at thousands of pieces.

For security reasons, radioactive sources are transported and stored in special containers which guarantee the minimum exposure to radiation. Such form of protection may attract scrap collectors. From the outside, the container may look as if it were made from high-cost materials, in particular, when its warning labels wore off or are gone. There were cases of persons who, unaware of the risk, in some cases innocent by-standards, tempered with the sources. Such tampering may often cause injuries or even death. In addition, there is a lot of radioactive waste around the world (typically generated by nuclear power plants or by production of weapons), spent atomic fuel and forms of radioactive substances not contained in shielding containers.

At the global scale, there are different programmes supporting countries in their operations in support for counteracting dissemination of radioactive materials. One of them is the Second Line of Defence – SLD Programme of the Department

of Energy (DoE) of the USA. The objective of the Programme is to detect and deter any illicit transport and transfer of nuclear and radioactive material using special RN-detecting instruments. The initiative has the following assets:

– Supporting research, development, production and logistics of special tools for RN detection;
– Organisation of free training and workshop events;
– Handing over, free of charge, of RN-detecting instruments and equipment.

Target users of the SLD Programme are:

– the Border Guard;
– the Customs;
– the Police;
– National Atomic Agencies.

At present, the programme is implemented in 24 countries: Afghanistan, Azerbaijan, Bulgaria, Croatia, the Czech Republic, Djibouti, Estonia, Germany, Georgia, Hungary, Israel, Iraq, Jordan, Lithuania, Mexico, Moldova, the Philippines, Poland, Romania, Slovakia, Slovenia, Tajikistan and the USA.

In the framework of the effort initiated by the Ministry of Internal Affairs and Administration of the Republic of Poland, a Task Force was formed for streamlining the rules for collaboration and managing operations on site of a terrorist incident in case of a CBRN agent involvement, by the virtue of the Decision No. 25 of the Chairman of the Interministerial Terrorist Threat Team of 26 March 2015. Its tasks included:

– revising the existing legal and organisational solutions related to the collaboration and managing terrorist events on site in case when CBRN agents are used and drafting proposed changes/ amendments in this respect;

– preparing recommendations on intensifying collaboration between competent agencies and institutions further to a terrorist incident in case of using a CBRN agent;

– drafting response procedures for competent agencies and institutions further to a terrorist incident in case of using a CBRN agent, taking into account their joint actions and optional scope of their operations depending on their risk assessment.

In view of potential terrorist threats with the use of chemical, biological, radiation or nuclear agents, states have or create their internal security system to counteract these threats or intervene when they take place. Anti-terrorist CBRN operations may be divided into:

– legislative and procedural operations;
– training;
– coordinating operations;
– acquisition of information;
– intervention;
– investigatory operations.

It is necessary to create or revise legislature translating into the organisation of the internal CBRN security system. Lawfully, the state should have a clear and structured division of competence and the algorithm for collaboration of entities and agencies responsible for CBRN anti-terrorist response. Imagine puzzles - with one element not fitting in, the whole image is spoilt. This comparison works here since any legal and procedural non-compliances may eventually result in an operational failure or its incomplete success.

The entire CBRN response system should be coordinated at the inter-ministerial level in order to monitor the system for potential gaps. A model solution is having the National CBRN Coordination Unit delivering the internal policy of the state also in terms of:

– coordinating all in-country CBRN operations;
– setting out the directions for preparing CBRN-response agencies and entities;
– analysing global CBRN incidents, taking into account response tactics used by the intervening agencies;
– supporting training of agencies and entities in CBRN threats and tactics of responding to CBRN incidents;
– collaborating with the academia and science also in the field of R & D programmes and EU projects in support for improving CBRN security;
– collaborating at the international level with institutions, organisations, states in the area of broadly understood CBRN.

An efficiently working CBRN response system also involves knowledge and skills of persons defined as CBRN forces. A broad-range, inter-ministerial training policy is required, unified for the purpose of joint operations of the agencies. The training programme should be a multi-module programme, taking into account groups responding to CBRN incidents i.e. the strategic, tactical and operating level. At each level, they should break down by the specialisation specified for an agency/entity in the national CBRN response system. Acquisition of information/intelligence operations are the necessary element that comes before an effective intervention or makes it possible with a potential prospect of preventing consequences of a CBRN terrorist attack. They are based on own or international sources of information.

An intervention is defined as taking physical actions oriented to the target location of an attack to prevent an actual CBRN crime. It includes: physical detention of the perpetrator, hazard detection, decontamination of detained persons and intervening officers/soldiers, isolation of the hazardous zone and evaluation operations.

In consideration of the most recent terrorist attacks or their failed attempts, with particular focus on mass events, etc., detailed procedures are required to achieve full CBRN security for large groups of people. It is impossible not to mention the importance of stressing security of mass events, important international meetings, conferences and religious events in the context of preventing terrorist CBRN

threats. Correct coordination and collaboration in ensuring anti-terrorist security is the key element of counteracting potential threats coming in the form of physical violence, weapons, CBRN factors and explosives used against people or property with violation of law. Improvement of the rules for coordinating and joint operations in providing anti-terrorist security of important international meetings and conferences and mass events, including improved response to CBRN hazards, is being implemented by Poland under the priorities of the 2015–2019 National Anti-Terrorist Programme.

When providing anti-terrorist CBRN security of important international meetings and conferences as well as mass events, it is necessary to:

– analyse risks, also on the basis of the data acquired by the Special Services, the Police and, potentially, any other competent agency in possession of information important due to the nature of an event;
– assess risks;
– indicate competent entity/agency, leading body or form a Task Force;
– define tasks and their completion dates.

If an entity, the leading body or forming a ministerial or inter-ministerial team competent for coordinating security of an event is appointed o formed, it is expected to perform the following:

– initiating collaboration with the organiser of an event, conference, meeting;
– analysing risk, assessing hazards;
– initiating collaboration with competent services according to the division of competence;
– analysing manpower and equipment necessary to deliver the task;
– preparing the schedule of works aim at ensuring CBRN security;
– developing a concept of operations (ConOps) containing, in particular:
  - assessment of the situation and an initial analysis of risks,
  - anticipated scenarios,
  - a threat assessment scheme,
  - operational goal/s and the method to achieve it/them,
  - manpower and equipment of all the services engaged to ensure CBRN anti-terrorist security,
  - tasks to persons responsible for specific area,
  - command and collaboration structure for the entities involved in the ConOps,
  - operation variants – defining the methods to achieve the planned goal of the operation,
  - organisation of connection,
  - organisation of the operational logistics, including equipment and operational technique, uniforms, transportation, medical service/care, providing for needs;

– arranging and structuring measures required to secure an event, preparing and introducing uniform response procedures for the case of a terrorist attack/threat;

– coordinates actions and flow of information related to the tasks to be competed when taking anti-terrorist CBRN operations;

– analysing and assessing own actions in terms of their effectiveness.

On the example of the Polish model of ensuring CBRN security of important international meetings, conferences and mass events by anti-terrorist measures, the role of the Police is to coordinate actions aimed at counteracting terrorist threats with the use of hazardous chemical compounds, biological material (bacterial and viral pathogens), radiation and nuclear material.

CBRN measures also include the following threat detection actions:

– detection of chemical (C) threats, with tactical operations led by the National Fire fighting Brigade, if necessary supported by the National Centre for Contamination Analysis (COAS);

– detection of biological (B) threats where the leading agency for tactical operations is the State Sanitary Inspection, if necessary, supported by the State Sanitary Inspection of the Ministry of Interior, the Epidemiological Response Centre of the Military Forces of the Republic of Poland and the National Fire Brigade;

– radiation and nuclear threats (RN) where the leading entity for tactical operations is the National Atomic Agency, if necessary supported by the National Fire Brigade, the Main Centre for Analysis and Contamination Centre (COAS), the Anti-Terrorist Operations Bureau of the Police HQs (BOA KGP).

The decontamination process is carried out by the National Fire Brigade with the support of the local governor who secures the quarantine site and any potential medical needs.

In addition, in the anti-terrorist security CBRN model, an important role is played by:

1. Analytical and information operations and operational and reconnaissance actions (the lead – the Internal Security Agency). The legal grounds for the Internal Security Agency taking the lead of the analytical and information operations and operational and reconnaissance actions to prevent and counteract terrorism stem from the provisions of art. 21 further to the provisions of art. 5 of the Internal Security Agency and the Intelligence Agency Law of 24 May 2002 (Dz.U. 2016 item 1897). Furthermore, art. 3 of the Counter-Terrorist Operations Law of 10 June 2016 (Dz.U. 2016, item 904) provides that the main responsibility of the Head of the Internal Security Agency is prevention of terrorist incidents. To this end, according to the provisions of art. 5 of the above-mentioned law, the Head of the Internal Security Agency coordinates analytical and information operations taken by institutions and agencies participating in the anti-terrorist security system for Poland who, according to the provisions of par. 3 of the above-

mentioned art. 5 are obligated to forward to the Internal Security Agency, without a delay, any information that serve conducting anti-terrorist operations classified according to the catalogue of terrorist incidents described in the regulation of the Minister of Internal Affairs and Administration of 22 July 2016 on the Catalogue of Terrorist Incidents (Dz.U. of 22 July 2016, item 1092). In addition, on the basis of art. 8 of the same law, he Head of the Internal Security Agency coordinates operational and reconnaissance actions taken by the security intelligence agencies, the Police, the Border Guard, the National Revenue Administration and the Military Police.

2. Warfare operations (the lead – the Police) – a set of operations delivered in a team by armed policemen, officers and soldiers equipped with specialist equipment, using anti-terrorist tactics with elements with the EOD tactics components such as defeating field obstacles and construction locks or neutralising explosive devices. These operations are oriented towards physical fighting terrorist attacks, in particular operations of a considerable degree of complexity as well as performed in the environment exposed to the impact of a chemical, biological agents, ionising and nuclear radiation and explosives.

3. VIP security ops (the lead – the Government Protection Bureau) to ensure security and protection of persons and objects of importance for the good and interest of the state, also in the context of the CBRN hazards.

4. EOD ops. (the lead – the Police) involving, in particular, locating, recognising, identifying, neutralising, removing, transporting and destroying improvised or plant- manufactured explosive materials and devices, taking into account the CBRN factors, which represent a threat for life, health and assets as well as the public security and public order and defeating construction locks and other obstacles by using explosives.

5. Information and press operations (delivered by the lead of the ops) aimed at running information policy, updating the public opinion on an on-going basis on methods of behaving in case of a potential CBRN terrorist incident (starting from notifying competent agencies about such suspicious incident and ending with the general guidelines on how to behave and proceed in specific cases). Through an appropriately run media policy resulting from collaboration of the public entities and the media, the general public may become a partner in recognising and identifying CBRN terrorist threats.

6. Rescue operations (the lead – the National Fire Brigade) understood as taking actions in order to protect life, health, property or the environment as well as liquidation of reasons for fire, natural disasters or another local threat.

7. Operations on the borders of the Republic of Poland (the lead – the Border Guard) by protecting the state border, organising and controlling the border traffic, issuing permits to cross the state border, preventing and detecting CBRN terrorist crimes and prosecuting their perpetrators, ensuring security on board of aircrafts carrying passengers.

The above-presented model solution for CBRN anti-terrorist protection of important international meetings and conferences as well as mass events was worked out on the basis of the experience from securing 2016 NATO Summi and the World Youth Days 2016 in Poland. A full set of innovative solutions has been developed as recommendations by "the Task Force for improving the rules for coordinating and joint operations to ensure anti-terrorist security of important international meetings and conferences and of mass investments, including in relation to the CBRN hazards" formed by the Chairman of the Inter-Ministerial Team for Terrorist Threats (Mr Mariusz Bałaszczak, Minister of Internal Affairs and Administration of the Republic of Poland) with a decision No. 29 of 23 September 2016. Owing to the commitment of the Polish Ministry of Internal Affairs, Poland succeeded in developing and introducing such an invaluable model of organisational and formal arrangements which has a huge impact on the CBRN security.

Many international CBRN agencies which specialise in different hazards work in support for international CBRN security, such as the International Atomic Energy Agency, the OPCW (the Organisation for Prevention of the Chemical Weapons), the international prosecution agencies (EUROPOL, INTERPOL) as well as units and work groups operating at the European Commission. In addition, there are also international initiatives for states, such as the GICNT – the Global Initiative for Combating Nuclear Terrorism. The nuclear terrorist threat is a global issue and an essential element affecting the process of creating internal and external policy of a state. Different states, depending on their potential and commitment, affect the global architecture of the protection system required for combating nuclear terrorism. Further to disproportionate capacities of states to counteract nuclear terrorism, manifesting themselves in the economic development and own expert and technical support, the idea of creating an alliance of countries to combat nuclear terrorism, called the Global Initiative. The Global Initiative was initiated by George W. Bush and Vladimir Putin on 15 July 2006 and consists in voluntary activity of states for the purpose of international cooperation oriented towards combating and counteracting the threat of global nuclear terrorism through:

– forming an union of countries engaged to deliver on the 8 key objectives enabling strengthening each of these countries in the field;

– voluntary actions in support for international exercise and exchange of information on best practices, full integration of independent efforts in combating nuclear terrorism;

– projects oriented towards improving collaboration of field and national units and the private sector with identification of nuclear terrorism combating tasks for each sector.

Appreciating the need for political commitment and systematic work, partner nations listed the objectives accepted by the engaged countries at the first Global Initiative meeting in September 2006, i.e.:

1. When necessary, management, control and physical protection related to the nuclear system and other radioactive materials should be improved.
2. Caring about ensuring security in case of nuclear applications for civil purposes.
3. Detection of nuclear and other radioactive materials by state institutions and entities which are links in the atomic chain to prevent illegal trading of such materials.
4. Preparing specialised institutions for finding, confiscating and controlled interception of nuclear materials and other radioactive materials as well as devices used for their production.
5. Counteracting sublimation of the environment related to the nuclear terrorism support.
6. Creating laws which allow for pressing charges against persons engaged in nuclear terrorism and holding them liable.
7. The ability to conduct investigations in case of crimes related to nuclear terrorism.
8. Observing protection of information related to the Global Terrorism in order to create a hermetic system for transferring knowledge which is essential in combating nuclear terrorism.

Creating and supporting international initiatives is a global pillar in support for actions taken by states on the local area where CBRN terrorism is combated.

CBRN terrorist threat may occur at any time; therefore, the services and agencies responsible for counteracting such attacks must remain vigilant and ready to respond. The above requires an efficient anti-terrorist CBRN system. Legal regulations providing for such incidents, international collaboration, some pre-defined manpower and equipment, including agencies and entities with appropriate technical background come as the core guarantor of CBRN security of the EU. Also note that, in case of such attack, one of the main objectives will be destabilising normal day-to-day life of the society. Building social awareness is of key importance in minimising potential consequences of such incident. It influences the process of overthrowing the stereotypes arising from lack of such awareness, which also translates into minimising symptoms of social destabilisation.

Read the message carried by a quote from the Pope John Paul II: "You must be self-demanding even if others are not demanding toward you".

Special dedication for M.A.M.