Rafał Kopeć
Pedagogical University in Krakow

THE THREAT OF MEGA-TERRORISM: AVAILABILITY, INHIBITORS AND MOTIVATION

Keywords: International Relations, terrorism, neapons of mass destruction, mega-terrorism, non-state actors

ABSTRACT: The prospect of weapons of mass destruction (WMD) terrorism poses a danger for contemporary societies. However, the incidents related to an application of weapons of mass destruction (that is, nuclear, chemical, biological and radiological weapons) by non-state actors are relatively rare. The aim of the paper is to present recent incidents and to estimate the threat from particular types of WMD. The author focuses both on the question of motivation to undertake these operations and on the problem of technological capabilities.

To sum up, the risk of a massive WMD terrorist attack should be perceived as quite moderate due to the technological barrier, but selective attacks carry a greater potential risk because of their higher probability and significant psychological effect.

1. INTRODUCTION

The threat of the so-called mega-terrorism (super-terrorism), that is, weapons of mass destruction terrorism, results from the combination of two security trends which are two distinctive factors of the post-Cold War era. The former is a growing threat of weapons of mass destruction itself, and the latter is a transformed nature of terrorism which significantly increases the probability of using weapons of mass destruction by terrorist organizations. The empowerment of international terrorist organizations accompanies this trend. These organizations have become a subject

of international relations due to the real capability to combat sovereign states[1]. The establishment of the anti-terrorist coalition after 9/11 attacks[2] actually enhanced the status of these organizations.

2. THE NATURE OF CONTEMPORARY TERRORISM

Contemporary terrorism, especially religiously motivated, is called postmodern terrorism. The type of violence is the crucial difference compared to the classic terrorism (generally politically motivated). Instead of instrumental violence, which is an enforcement method to carry out a given political objective (most often government concessions), postmodern terrorism applies expressive violence. The act of violence is an end in itself[3]. The pursuit of killing a vast number of the "infidel" also matters in case of faith-based terrorism[4]. Accidental victims are no longer perceived as an inevitable sacrifice, essential to achieve the goal, however unwanted. In the past, the public opinion support (e.g. support by a country's population) served as a legitimacy factor, which excluded mass casualties. Nowadays, postmodern terrorism does not apply such methods to reduce or even eliminate accidental victims as bomb warning made verbally over the phone. An attack itself was a sufficiently clear message and victims could interfere the process of acquiring public opinion support.

At present, the situation is the opposite – the maximization of the number of victims is an expected factor. It is because postmodern terrorism does not require any public opinion support – religion is a reference point. A religious character of the attacks is – in their authors' opinions – an adequate justification, so there is no need to search for any additional

[1] A. Bógdał-Brzezińska, *Porządek międzynarodowy w perspektywie badań angielskiej szkoły stosunków międzynarodowych*, in: R. Kuźniar (Ed.), *Porządek międzynarodowy u progu XXI wieku. Wizje – koncepcje – paradygmaty,* Warszawa 2005, p. 309.

[2] *International Contributions to the War Against Terrorism*, available at: http://www.defense.gov/news/Jun2002/d20020607contributions.pdf, (accessed 28.03.2012).

[3] Ł. Kamieński, *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych*, Krakow 2009, p. 194.

[4] J. Pawłowski, *Broń masowego rażenia orężem terroryzmu*, Warszawa 2004, p. 19–20.

motivation in this earthly world[5]. According to Joseph Nye contemporary terrorism is based on mass casualties, whereas terrorism in the 20th century tended rather to acquire mass audience[6]. Certainly, modern communication technologies, first of all the internet, make it possible to increase the number of the audience more than ever before. However, it is not necessary now to trigger reactions between terrorists, public opinion and the government. Both, intimidating the society and the impact of the so-called theater of terror still exist, but striking fear into the society is no longer a means to influence the government. An objective of conventional terrorism was to exert an influence on the government to change its politics (or even eliminate it), whereas the society served as a means of communicating ideas and a pressure element. On the contrary, the postmodern terrorism's objective is the whole society as not deserving any respect (for example representatives of a different faith or even of a faction within a faith – as in the Shia-Sunni clash – or the condemned "godless and decadent" Western societies). The maximization of the number of victims has become thus a desirable feature of postmodern terrorist attacks.

Herfried Münkler writes about recent tendencies breaking the self-limitation of terrorism, which used to restrain the usage of weapons of mass destruction. These tendencies include:[7]

- the internalization of terrorism; this trend had begun in the '60s and boosted in the '90s; the internalization of terrorism results in a dispersion of a violence circle (for example passengers of an attacked plane come from different countries), which makes it impossible to select victims – it is the first step to spark the spiral of violence;
- religious fundamentalism as a crucial part of terrorists' motivation; this kind of terrorism does not address public opinion in order to win the society over to terrorists' side (like conventional terrorism, e.g. separatist terrorism), which could result in the drop of the

[5] H. Münkler, *Wojny naszych czasów*, Krakow 2004, p. 147–149.

[6] J.S. Nye jr., *Soft Power. Jak osiągnąć sukces w polityce światowej*, Warszawa 2007, p. 52–53.

[7] H. Münkler, *Wojny naszych czasów…*, op.cit., p. 136–138, 142–143, 147, 149.

number of victims or in their selection; the terrorism driven by religious fundamentalism strives for the maximization of the number of victims among the society seen as an enemy, alternatively for the establishment of a new community (e.g. a new Islamic community which is convinced that an effective struggle against the West is possible);

– terrorism is no longer an initial stage before any further action (e.g. as a preparation for an uprising – it could reduce the number of victims in order to win any supporters over), however, it is the strategy itself, which justifies the maximization of the number of victims;
– the conflict between a post-heroic mentality attributed to the West and heroic mentality represented by terrorist groups; this factor explains wide-spreading suicide attacks, which are extremely difficult to defend from (there is a great variety of ways of attacks, as it is not necessary to consider any way of escape); what is more, a suicide attack notifies of the determination of its author, especially if it is addressed to post-heroic societies (a psychological impact caused by this type of message is greater in post-heroic societies);
– taking advantage of media revolution: a requirement of getting through media hype induces to apply more and more spectacular operations in order to "produce" terrifying pictures; an attack with the use of weapons of mass destruction perfectly meets this requirement;
– the exclusion of a compromise: there is no room for negotiations, when terrorists leave a picture of violence itself, without explaining a reason of an attack or making demands; any compromise is excluded in advance; an additional feature of this strategy is an ambiguous aim – it is not about meeting any specific demand, which could close a terrorist campaign, but it is about causing an overwhelming fear and feeling of the permanent lack of security.

3. THE APPLICATION OF WEAPONS OF MASS DESTRUCTION BY TERRORISTS

These circumstances may enable the terrorists to apply weapons of mass destruction. These types of weapons appear to be tailor-made in order to maximize the number of victims and the scale of fear. Consequently, a strong motivation to acquire and apply the weapons of mass destruction by terrorist groups can be supposed. However, the analysis of terrorism history demonstrates that the application of weapons of mass destruction by terrorists is rather an exception than the rule.

According to the study by National Defense University in 2001 there were 180 cases of illicit (terrorist or criminal) biological agent activity in the 20th century. Only 21 of these cases involved its real use, while the threats only were among a vast majority of cases.

Table 1. Confirmed cases of illicit biological agent activity

Type	Terrorist	Criminal	Other/Uncertain	Total Cases
Acquire and Use	5	16	0	21
Acquire	3	7	2	12
Interest	6	4	0	10
Threat/Hoax	13	29	95	137
Total Cases	27	56	97	180

Source: W.S. Carus, Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900, Washington 2001, p. 8.

Over the recent years (since the '80s) one can indicate the following cases of applying biological weapons by terrorist or similar groups:

– an attempt to poison people at The Dalles town in the United States in 1984 by the members of the Neo-Sannyas sect (its leader was a Hindu guru Bhagwan Shree Rajneesh). The purpose of the attack was to take over the reins of local authority by changing the council election's results (it was presumed that sick inhabitants could not take part in the election). It should be noted that relations between the local community and the members of the sect were extremely tense. Salad bars were the target of the attack. It ended

with poisoning of 751 people, but there were no fatalities. The epidemic was recognized as group food poisoning on the ground of natural reasons and after one year it was bound with the sect activity[8].

– Larry Wayne Harris, the member of the American neo-Nazi group Aryan Nations, acquired from a biochemical company the freeze-dried Yersinia pestis, the pathogen that caused bubonic and pneumonic plague in 1995. Harris claimed that the material was necessary to conduct an experiment, which would be the background of his book (a kind of a manual describing the methods of protecting against biological attacks), since he was afraid of a biological attack by Iraq. The information about the transaction was found out by the health care service and then by federal authorities. Harris was arrested, finally it occurred that he had possessed a plague bacteria legally. He was only accused and convicted of a fraud concerning the acquisition and was sentenced to 18 months probation and 200 hours of community service. At his own expense he published a book Bacteriological Warfare: A Major Threat to North America. The result of his activity was the enactment of a law imposing on government institutions an obligation of more scrutinous monitoring of deliveries containing infectious agents[9].

– Biological attacks by the Aum Shinrikyō sect (Eng. Supreme Truth, established by Shōkō Asahara). The sect tried to acquire an Ebola virus – its members came with this purpose to Zaire in 1992, officially with a humanitarian aid[10]. Aum Shinrikyō made a few attempts to apply biological weapons. In 1990 it spread a botulinum toxin out of a vehicle around the Japanese parliament. In 1993 the sect members tried to disturb the wedding ceremony of the Prince

[8] J. Kastner, *Food and agriculture security: an historical, multidisciplinary approach*, Santa Barbara 2011, p. 69.

[9] W.S. Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*, Amsterdam 2002, p. 152.

[10] M. Leitenberg, *The Experience of the Japanese Aum Shinrikyo Group and Biological Agents*, http://www.fas.org/bwc/papers/aumpap.htm, (accessed 14.03.2012).

of Japan by spreading a botulinum toxin. The same year the sect conducted an anthrax attack in Tokyo, spreading it from a building roof. The ineffectiveness of those attacks drew the sect's attention to chemical weapons[11].

– Anthrax terrorist attacks in the United States in the period of 16th September to 25th November 2001. Letters containing anthrax spores were sent to media (NBC News and New York Post) and several important institutions (e.g. Senate). It was the first time anthrax was used as a biological weapon. There were 22 people poisoned (11 were infected by cutaneous anthrax – on the skin – and 11 by pulmonary anthrax). 5 out of them died – all in consequence of pulmonary infection[12]. It was a well-prepared attack, what an accurate adjustment of physical characteristics demonstrated – micro-holes in anthrax-containing envelopes were about 100 microns in diameter, powder fraction was about 50 microns, and anthrax spores between 4 and 6 microns. Hence every single move of an envelope resulted in spreading spores[13]. Contaminated deliveries were sent also to the US embassy in Vilnius and to the editor-in-chief of the Pakistani paper Daily Jang[14].

The official investigation was closed in February 2010. The only official suspect was Dr. Bruce Ivins, a microbiologist at the U.S. Army Medical Research Institute of Infectious Diseases in Fort Detrick. Ivins committed a suicide on 29th July 2008, taking an intentional overdose of Tylenol after learning that formal accusation of him is possible. However, the results of the investigation are very questionable – evidence against Ivins was circumstantial, his suicide could be related to the fear of his unusual sexual preference disclosure. Moreover, possible initiators of the attack were not found and the investigation did not reveal any connections between attackers and foreign terrorists groups[15]. These relations seem to be pos-

[11] J. Pawłowski, *Broń masowego rażenia orężem…*, op.cit., p. 95.

[12] B. Michailiuk, *Broń biologiczna*, Warsaw 2004, p. 16.

[13] J. Pawłowski, *Broń masowego rażenia orężem…*, op.cit., p. 17.

[14] Ibidem, p. 99.

[15] K. Kęciek, *Kto wysyłał wąglika?*, http://www.przeglad-tygodnik.pl/pl/artykul/kto-wysylal-waglika, (accessed 14.03.2012).

sible because of the date of the attacks – shortly after an 9/11 attack. Furthermore, the information about biological weapons (e.g. a manual of spreading agents by means of agricultural aircrafts) was found in personal belongings of one of the 9/11 terrorists[16]. What is more, during the War in Afghanistan the Northern Alliance soldiers found in al-Qaeda barracks in Kabul an instruction to produce ricin[17].

The use of chemical weapons for terrorist purposes concerns actually one case, however a very serious one, that is, the Tokyo underground attack by the Aum Shinrikyō sect on 20th March 1995. The terrorists used liquid sarin placed in plastic bags and lunch boxes. At prearranged time the attackers, who were in 3 different subway trains, punctured the sarin packages with umbrella tips. The attack was launched during the morning rush hour. As its result 13 people died and nearly 6 thousands were seriously poisoned. In fact, the main purpose of the attack was not to cause mass casualties, but to get rid of policemen from the Police Headquarter, who had used these subway lines[18]. Earlier, in 1994, the sect had carried out an unsuccessful attack on judges in order to prevent the court from delivering a prospective verdict in trial over the fraud case, which was unfavorable for the sect. As a result of the so-called Matsumoto incident 8 accidental people died and over 200 were injured.

A chemical attack was also planned by Ramsi Yousef, an organizer of the World Trade Center bombing in 1993. He intended to use cyanide as a part of a self-made explosive device, however, its construction details and the mode of the action are not clear. The idea of using cyanide was eventually rejected due to high costs (the attackers were forced to reduce the total cost of preparing the device to only 15 thousand US dollars)[19]. Finally, the attackers collected and detonated urea nitrate (with nitroglycerin to boost the blast) conventional explosive device. 6 people were killed and more than 1 thousand were injured in the attack.

---

16 B. Michailiuk, *Broń biologiczna…*, op.cit., p. 17.

17 J. Pawłowski, *Broń masowego rażenia orężem…*, op.cit., p. 74.

18 Ibidem, p. 42.

19 E. Croddy, C. Perez-Armendariz, J. Hart, *Broń chemiczna i biologiczna – raport dla obywatela*, Warszawa 2003, p. 94.

Any case of applying nuclear and radiological weapons for terrorist purposes has not been identified so far. The most important incident related to this sort of weapons took place in Moscow on 23th November 1995. Shamil Basayev, the leader of the Chechen rebel movement, announced on the NTV television that he had buried a container holding radioactive cesium-137 in the Moscow's Izmailovsky *Park. The reporters discovered a canister – indeed, it contained cesium-137 (the object was* a piece of an X-ray machine stolen from the hospital in Budennovsk). However, there was not any detonator and the amount of cesium-137 was rather small. The incident was not an attempt of a radiological attack, but a message to the Russian authorities, saying that Chechen rebels possess radiological materials and are ready to use them [20].

Any attack on a nuclear power plant or radioactive waste store in order to cause radioactive pollution has not been recorded yet even though this form of weapons of mass destruction terrorist attack has been seriously considered for more than a decade[21]. After 9/11 attacks the possibility of making use of a hijacked passenger airliner by terrorists drew public attention. Existing nuclear power plants were constructed in order to withstand a light aircraft or jet fighter accidental impact (concrete reactor domes were successfully tested in the United States and Japan by the F-4 fighter hitting in at 800 km/h)[22]. No one imagined that much bigger aircrafts were a real danger.

---

[20] G. Cameron, *Nuclear Terrorism: A Threat Assessment for the 21st Century*, London 1999, p. 143.

[21] However, there were three incidents related to the infiltration of security systems of the South Afrika's Pelindaba Research Center. Details of these incidents were not made public, but it is known that the most serious one took place on 8th November 2007. The team of four armed men deactivated several layers of security systems, shot an off-duty emergency services officer and stole a computer from the emergency control center. At the same time, the second group of attackers failed in an attempt to break in from western perimeter. It is probable that the coordinated attack targeted at weapons-grade nuclear material storage. M. Zenko, "*A Nuclear Site Is Breached*" – *South African Attack Should Sound Alarms*, available at: http://belfercenter.hks.harvard.edu/publication/17791/nuclear_site_is_breached.html, (accessed 29.10.2012); *Another Infiltration Reported at South African Atomic Site*, available at: http://www.nti.org/gsn/article/new-infiltration-reported-south-african-atomic-plant/, (accessed 29.10.2012).

[22] W.B. Pietrzak, *Terror atomowy – czy tylko kwestia czasu?*, "Raport – Wojsko Technika Obronność", 2004, No. 2, p. 39.

In a hypothetical scenario described in the scientific weekly magazine New Scientists a passenger airliner Boeing 747 with 200 thousand liters of fuel stroked in radioactive waste tanks in Sellafield in Northern England. The accident could result in releasing 1500 kilograms of radioactive cesium-137. Due to the high population density of surrounding areas it could end in 2 million people sick with thyroid cancer (to compare, after the Chernobyl disaster there were 11 thousand of these cases). The number of possible fatalities is difficult to estimate, but it could be around several thousand.[23]

Security measures to counter a nuclear power plant attack refer to 3 major concerns:[24]

– to control nuclear chain reaction,
– to assure that a reactor core does not lose its coolant and "melt down" from the heat, even if chain reaction stops,
– to protect storage facilities for radioactive spent nuclear fuel.

In 1967, the American Atomic Energy Commission (AEC) instituted a rule related to the robustness of nuclear power plants. It specified that nuclear power plants are "not required to provide for design features or other measures for the specific purpose of protection against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person, or (b) use or deployment of weapons incident to U.S. defense activities."[25]

After 9/11 attacks the Nuclear Regulatory Commission (NRC), successor of AEC, focused on the vulnerability of nuclear power plants to terrorist attack and established new security requirements. NBC approved its final rule on 29th January 2007 (effective since 18th April 2007). Although specific details were not released to the public, the rule increased the number of assumed attack scenarios in general and revised the threat

[23] P. Gawliczek, *Terroryzm z wykorzystaniem broni masowego rażenia (megaterroryzm) jako zagrożenie asymetryczne. Formy przeciwdziałania*, Warszawa 2007, p. 88.

[24] M. Holt, A. Andrews, *Nuclear Power Plants: Vulnerability to Terrorist Attack*, CRS Report for Congress, Washington 2007, p. 1, 4–6.

[25] Ibidem, p. 2.

posed by expanded capabilities of adversaries. It implicated the introduction of more detailed procedures, for example the extension of the range of vehicles, which require special entry permits (e.g. water tanks).[26]

These regulations did not involve security measures directed at a hijacked airliner attack, which provoked public criticism. The main concern was the prospect of a big airliner (especially filled up with fuel) striking into the containment building and consequently a core melt-down or reactor's fire. It could result in widespread radiation exposure. However, the specialists' opinions about the seriousness of that threat were mixed[27]. NRC rejected the proposal of the Union of Concerned Scientists – nuclear power plants would be surrounded by aircraft barriers made of big steel beams and cables (the so-called "beamhenge" concept[28]). NRC experts argued that nuclear power plants are already prepared for that kind of attack to some extent (security measures involve only the mitigation of the effects of aircraft crashes instead of their complete prevention). They also pointed out that active protection against airborne threats is addressed by other federal organizations, including the military[29] and that nuclear power plants are a difficult target because of their low profile and relatively small size. According to Nils Diaz, former NRC Chairman, even in case of striking the reactor building "the likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low."[30]

In 2007, NRC proposed new rules for new certified designs or new reactor licenses using uncertified designs. Nuclear power plant's design features, capabilities, and operations should be able to avoid or mitigate the effect of a big airliner crash. The new rules, taking into account the effect of the impact of a large, commercial aircraft were approved on 17th February 2009. Based on them the Westinghouse company redesigned the

---

26 Ibidem, s. 1.

27 Ibidem, s. 1.

28 *For more information about the project, please read: Bridging the Gap Between Nuclear Dangers & a Safe, Sustainable Future*, available at: http://www.committeetobridgethegap.org/beamhenge.html, (accessed 25.08.2012).

29 M. Holt, A. Andrews, *Nuclear Power Plants Security…*, op.cit., p. 3.

30 Ibidem, p. 4.

AP1000 reactor (the reactor was previously certified, so the upgrading was not required by NRC). The new design included adding steel plates inside and outside of the reactor's concrete containment structure in order to increase the protection level against the large aircraft penetration.[31]

Other scenarios of a nuclear energy facility terrorist attack are taken into account. Due to that possible incident nuclear sites are subject to exceptionally rigorous security measures. For instance, American nuclear power plants are divided into three security zones:[32]

- buffer region,
- protected area (restricted access, only for a part of employees, monitoring of visitors) – vital area (more strict protection, additional access requirements).

Each American nuclear power plant has to conduct security exercises every three years. The test is a kind of a simulated attack („force-on-force exercises") – both plant's guard force and mock adversary force are equipped with weapons with laser combat simulation system (they also wear laser sensors to indicate hits). It is also possible to simulate other weapons and explosives or specific damages. Nuclear plant guards know neither exact time of an attack's simulation (they are only informed that an attack occurs during a specific period) nor an attack scenario. They are obligated to maintain normal operating activities of the plant. The program of force-on-force exercises began in 2004.[33]

The first three-year cycle of exercises included 172 force-on-force inspections in all 64 American nuclear plants during the period from 2004 to 2007. Two of them ended in simulated destruction of the vital infrastructure (it could cause large-scale radioactive release in reality). The exercises met with criticism, when information about managing the adversary force by the Wackenhut company (which is a provider of security service for several nuclear plants at the same time) came to light. This conflict of interest resulted in a distortion of exercises' scores. Finally, Wackenhut was excluded from the security contracts when the incident

[31] M. Holt, A. Andrews, *Nuclear Power Plants: Vulnerability*…, op.cit., p. 4–5.
[32] Ibidem, p. 1.
[33] M. Holt, A. Andrews, *Nuclear Power Plants Security*…, op.cit., p. 5–6.

with Peach Bottom nuclear plant guards sleeping on duty was revealed (the video recording showing sleeping guards was done by two ex-workers and presented in a local TV)[34].

The new security measures were approved by NRC 17th December 2008 as a result of the analysis of these exercises. The measures notice the following:[35]

- preventing plutonium-bearing mixed oxide fuel from theft or diversion,
- preventing digital computer and communication systems and networks from cyber attacks,
- preparation of the strategies of responding to an aircraft attack (e.g. a pattern of conduct in case of warning of an aircraft attack and to mitigate the effects of large explosion and fires),
- implementing more rigorous programs for authorizing access (including enhanced psychological assessments and programs of behavioral staff observation),
- modification of the requirements in order to personnel training (including more rigorous physical fitness standards),
- implementing physical security requirements (including ensuring the availability of backup security command center and uninterruptible power supplies to detection systems, enhancing video capability, protection from waterborne vehicles ramming into the plant gate).

4. THE INHIBITORS OF THE USE OF WEAPONS OF MASS DESTRUCTION BY NON-STATE ACTORS

The weapons of mass destruction, in spite of their numerous advantages as a weapon of terror, have not been widely applied by terrorist organizations. While the nature of postmodern terrorism indicates that the lack of motivation is not the root of the problem (WMD are a highly

[34] Ibidem, p. 6–7.
[35] Ibidem, p. 9.

desirable fighting method), we can attribute this situation to the difficulty to acquire militarily usable WMD.

Fruitless efforts of the Aum Shinrikyō sect (beside a high level of motivation and huge financial and organizational capabilities[36] the sect failed to apply biological weapon effectively) lead to the conclusion that a massive biological terrorist attack is a formidable challenge. Production of biological agents is not an insurmountable obstacle for non-state actors[37], but their preparation in such way that they would be applied on a massive scale. Another inhibitor is a necessity to develop an efficient way of releasing pathogens. Many ways of releasing them are not adequate in order to carry out a biological attack on a large scale, such as insects (they are unpredictable), poisoning water supplies (it requires a large amount of pathogens, which could be detected by water filter systems[38]), contaminated food (pathogens can be neutralized in the food production process), an infected person (in this case, the most suitable pathogen is smallpox virus due to its contagiousness and mortality; however, it is extremely difficult to obtain it as the only pathogens are stored in the laboratories in Atlanta and Koltsovo[39]).

[36] However, it is worth mentioning that there were more chemists and physicists then microbiologists in the sect. K. Langbein, Ch. Skalnik, I. Smolek, *Bioterroryzm*, Warszawa 2003, p. 39.

[37] The provocation by the "Sunday Times" journalist (purchasing bacteria in 1998) and the simulation of building a biological weapon factory from off-shelves materials carried out by Pentagon in 1998–2000 proved an easy access to the material used to produce biological weapons. K. Langbein, Ch. Skalnik, I. Smolek, *Bioterroryzm…*, op.cit., p. 141–143.

[38] The effect of a hypothetical chemical or biological attack against water supply system is reduced by the need to dilute a chemical/biological agent. What is more, chlorination and ozonation can neutralize many pathogens. The water quality is constantly monitored and waterworks are under surveillance. E. Croddy, C. Perez-Armendariz, J. Hart, *Broń chemiczna i biologiczna…*, op.cit., p. 111–116.

[39] In 1980, the World Health Organization announced an eradication of smallpox virus. There are only two official repositories of smallpox in the world: US Centers for Disease Control and Prevention in Atlanta (USA) and the State Research Center of Virology and Biotechnology VECTOR in Koltsovo (near Novosibirsk, Russia). Despite the initial plan to destroy this virus, the need to preserve it in case of a hypothetical epidemic in future was recognized (a hypothetical scenario assumes a biological attack

Using an aerosol is the optimal way to release pathogens. There are two kinds of aerosols: liquid (it is less efficient but easier to prepare) and gas (it demands dry spores, which are very difficult to prepare. For example, the scientists in Hussein's Iraq were not able to break through this technological barrier[40]). The requirements for preparation an anthrax weapon (which appears to be one of the most effective biological weapons for terrorist purposes[41]) can serve as an example of difficulties of a biological warfare. It is necessary to grow highly virulent strain and its adequate preparation (grinding material and adding antistatic agents). Then the spores can be used to make a highly concentrated aerosol form. None of these steps is easy to fulfill.

Another obstacles in the process of preparing and carrying out an attack are the difficulty with the ready-to-use weapon storage (many biological materials undergo the inactivation relatively rapidly), and the risk of the infection both in the production process and as a result of an attack[42].

A large-scale biological attack carried out by a non-state actor are seems to be unlikely. A selective attack (similar to 2001 anthrax attacks) is more probable. A direct attack (a selective transmission of a biological agent) would not result in the large number of victims, but an attack's potential psychological impact can be enormous.

The forecast of a possible chemical attack by a non-state actor is similar as in case of a biological weapon. Even the large-scale attack by the

---

carried out by a state or an organization which preserves smallpox virus secretly). E. Croddy, C. Perez-Armendariz, J. Hart, B*roń chemiczna i biologiczna…*, op.cit., p. 97–102.

[40] K. Langbein, Ch. Skalnik, I. Smolek, *Bioterroryzm…*, op.cit., p. 146–148.

[41] Anthrax spores are highly survivable and capable of withstanding many countermeasures. Pulmonary infection is extremely dangerous. Only a quick diagnosis gives a chance to survive, but it is not an easy task to distinguish anthrax from other, more common cases of pulmonary illness. As the result, the majority of infected persons cannot avoid delays in diagnosis and treatment. An antibiotic therapy can be effective, but only on the condition of an early diagnosis.

[42] The Japanese Changtech biological attack (1941) can illustrate this danger. It ended not only in about 10 thousand Chinese deaths, but also 1700 Japanese. J. Pawłowski, *Broń masowego rażenia orężem…*, op.cit., p. 90–91.

Aum Shinrikyō sect does not significantly change this prediction. Admittedly, this case indicates that without any assistance from a country a non-state organization could acquire a large amount of chemical precursors, but finally the technological barrier would not be broken down. In spite of the access to well-equipped laboratories, highly trained personnel, and substantial financial resources the sect produced sarin of an insufficient quality, whereas different chemical agents (e.g. VX) were turned down as too complicated[43]. What is more, the outcomes of the Tokyo attack were limited due to a crude method of releasing an agent which was applied. The construction of a chemical agent releasing device, which can be able to cause mass casualties, is more challenging than the preparation of a chemical agent (this is the same problem as in the case of a biological weapon). Consequently, the most serious WMD terrorist attack resulted in 13 deaths only. Compared to the effects of a conventional terrorist attack the results of applying WMD by a non-state actor seem to be very unextraordinary. Obviously, psychological results of a possible chemical attack carried out by a non-state actor are to be taken into consideration, however, limited physical effects make the "weapon of mass destruction" term paradoxically quite inadequate.

The evaluation of a radiological and nuclear weapons threat is complicated because of the fact that these kinds of weapons have been never adopted by any non-state actor. A radiological weapon is undoubtedly easier accessible than a nuclear weapon, however, even in this case the construction of a radiological dispersal device capable of causing mass casualties is an immeasurably difficult task. It is because of the requirement to acquire an appropriate amount of a fissile material and to develop an effective way to release contamination. An additional problem is the radioactivity of fissile materials, which bring a risk during transport and

[43] Actually, each kind of a chemical weapon suffers a serious setback in order to be applied as a weapon of massive attack by a non-state actor. The production of tabun, for example, is hindered by the excretion of toxic prussic acid; production of sarin, soman, and VX requires high and accurately controlled temperature, additionally corrosive substances are excreted; mustard gas and lewisite can be relatively easily produced, but their components are hardly accessible due to the implementation of the Chemical Weapons Convention. J. Pawłowski, *Broń masowego rażenia orężem…*, op.cit., p. 43.

operating. It involves radiation hazard for staff. Moreover it increases the possibility of being unveiled by state service. For these reasons, the most probable option of a radiological weapon terrorist application is the detonation of a ready radioactive element[44]. Radioactive isotops are also much more hard to reach compared to chemical and biological materials, let alone conventional explosive materials. It is due to their relative low prevalence and trade control measures as well (even if these measures are insufficient, they are an additional obstacle to acquire radioactive materials).[45]

Considering a nuclear weapon, terrorist organizations focus probably on acquiring a ready-to-use weapon. The most possible scenario assumes a loss of the arsenal control by a nuclear state[46]. Terrorist organizations tend to seize a ready-to-use (or almost ready) weapon[47] instead of getting components, knowledge or technologies (what is characteristic for threshold states). The technological barrier related to the nuclear weapon construction seems to be too difficult to overcome for a non-state actor[48]. A uranium gun-type nuclear weapon is characterized by the relatively low level of technological sophistication what makes it moderately difficult to

---

[44] M. Witczak, B. Kot, *Ocena możliwości użycia broni masowego rażenia w przyszłych konfliktach zbrojnych i wynikające z niej zagrożenie dla terytorium Polski*, "Myśl Wojskowa" 2005, No. 6, p. 82.

[45] For more information about the radiological attack estimated threat, please read: P. Gawliczek, *Terroryzm z wykorzystaniem broni masowego rażeni*a…, op.cit., p. 23.

[46] Small size nuclear warheads could be very useful in this case. They were designed in the United States (W-54 warhead, which was an element of the Davy Crockett system; it was a low yield tactical nuclear weapon, intended to be used in a nuclear battlefield; *The Davy Crockett*, http://www.brookings.edu/projects/archive/nucweapons/davyc.aspx, (accessed 15.04.2012) and in the Soviet Union. In USSR suitcase nuclear bombs were developed (weight: about 30–40 kg; yield: about 1 kiloton of TNT), destined for the destruction of crucial elements of infrastructure. During the Boris Yeltsin's presidency a special commission was established in order to investigate circumstances concerning suitcase nukes. The commission was headed by General Alexander Laded, Secretary of Security Council. It unveiled that only 48 bombs out of 134 fabricated were found (W.B. Pietrzak, *Terror atomowy…*, op.cit., p. 38).

[47] J. Pawłowski, *System przeciwdziałania rozprzestrzenianiu broni masowego rażenia*, Warsaw 2008, p. 30.

[48] P. Gawliczek, *Terroryzm z wykorzystaniem broni masowego rażenia…*, op.cit., p. 19.

design and produce, but it requires a large amount of highly enriched uranium (at least 50 kg for each device)[49]. By contrast, a plutonium-fueled implosion-type weapon is a distinctly complex device.

Marcin Kloske indicates the contradiction in the requirements related to a nuclear weapon if it would be used by a non-state actor. According to him, an essential requirement is its small linear dimension, the simplicity of its design and the easiness of manufacturing it. On the other hand, the possibility to apply poor quality plutonium or even used nuclear fuel is expected. Living up to these contradictory expectations (a high yield and poor quality fissile material) is objectionable or even impossible. As a result, the prospect of building own nuclear weapon by terrorist organizations is rather not upon us today.[50]

5. CONCLUSION

The risk of a WMD terrorist attack should be perceived as quite moderate if taking into consideration both a relatively small number of WMD applications by non-state actors and the technical requirements indicated above. However, a possible WMD acquisition by a non-state actor (especially when it comes to chemical and biological weapons) has to be taken into account. Two key factors indicate this possibility: contemporary, postmodern terrorism provides the motivation to include WMD in the catalogue of terrorist methods and there is a potential of the relatively easy production of some kinds of WMD. It is necessary though to consider the distinction between the ability to produce WMD and to carry out a massive attack. Carrying out a massive attack is determined by the proper preparation of an agent and development of an efficient way to release it. The technological barrier related to these requirements is still extremely challengeable for non-state actors.

---

[49] J. Kubowski, *Broń jądrowa. Fizyka, budowa, działanie, skutki, historia*, Warszawa 2008, p. 47.

[50] M. Kloske, *Możliwość zastosowania broni masowego rażenia przez organizacje terrorystyczne*, "Myśl Wojskowa" 2006, No. 1, p. 94.

Selective attacks carry a greater potential risk because of their higher probability. The extent of losses, which might be the result of selective attacks, must be relatively small, but their psychological effect can be significant and can lead to very painful consequences. The nature of WMD favors the psychological effect because contemporary societies are not "familiar" with the way WMD works (compared to the conventional weapons). What is more, the results of using weapons of mass destruction, which make them abhorrent and bring condemnation of their users, can intensify the psychological effect.

BIBLIOGRAPHY

Another Infiltration Reported at Soyth African Atomic Site, The Nuclear Threat Initiative, available at: http://www.nti.org/gsn/article/new-infiltration-reported-south-african-atomic-plant/, (accessed 29.10.2012).

Bell K., Gray Ch.H., Mentor S., *Understanding Postmodern Terrorism*, in: Cummings B.L. (Ed.), *Beyond the Campaign: the Future of Countering Terrorism, Council for Emerging National Security Affairs*, New York 2004.

Bógdał-Brzezińska A., *Porządek międzynarodowy w perspektywie badań angielskiej szkoły stosunków międzynarodowych*, in: Kuźniar R. (Ed.), *Porządek międzynarodowy u progu XXI wieku. Wizje – koncepcje – paradygmaty*, Warszawa 2005.

Bridging the Gap Between Nuclear Dangers & a Safe, Sustainable Future, Committee to Bridge the GAP, available at: http://www.committeetobridgethegap.org/beamhenge.html, (accessed 25.08.2012).

Cameron G., *Nuclear Terrorism: A Threat Assessment for the 21st Century*, Macmillan Press Ltd, London 1999.

Carus W.S., *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*, National Defense University, Center for Nonproliferation Research, Washington 2001.

Carus W.S., *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*, Fredonia Books, Amsterdam 2002.

Croddy E., Perez-Armendariz C., Hart J., *Broń chemiczna i biologiczna – raport dla obywatela*, Warszawa 2003.

Gawliczek P., *Terroryzm z wykorzystaniem broni masowego rażenia (megaterroryzm) jako zagrożenie asymetryczne. Formy przeciwdziałania*, Warszawa 2007.

Holt M., Andrews A., *Nuclear Power Plants Security and Vulnerabilities, CRS Report for Congress, Congressional Research Service*, Washington 2009.

Holt M., Andrews A., *Nuclear Power Plants: Vulnerability to Terrorist Attack, CRS Report for Congress, Congressional Research Service*, Washington 2007.

International Contributions to the War Against Terrorism, Department of Defense, available at: http://www.defense.gov/news/Jun2002/d20020607contributions.pdf, (accessed 28.03.2012)

Kamieński Ł., *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych*, Krakow 2009.

Kastner J., *Food and agriculture security: an historical, multidisciplinary approach, ABC-CLIO,* Santa Barbara 2011.

Kęciek K., *Kto wysyłał wąglika?, "Przegląd"*, available at: http://www.przeglad-tygodnik.pl/pl/artykul/kto-wysylal-waglika, (accessed 14.03.2012).

Kloske M., *Możliwość zastosowania broni masowego rażenia przez organizacje terrorystyczne*, "Myśl Wojskowa" 2006, No. 1.

Kubowski J., *Broń jądrowa. Fizyka, budowa, działanie, skutki, historia*, Warszawa 2008.

Langbein K., Skalnik Ch., Smolek I., *Bioterroryzm*, Warszawa 2003.

Laquer W., *Postmodern Terrorism: New Rules for an Old Game*, "Foreign Affairs", 1996, Vol. 75, No. 4.

Leitenberg M., *The Experience of the Japanese Aum Shinrikyo Group and Biological Agents, Center for International and Security Studies, University of Maryland*, http://www.fas.org/bwc/papers/aumpap.htm, (accessed 14.03.2012).

Michailiuk B., *Broń biologiczna*, Warszawa 2004.

Münkler H., *Wojny naszych czasów*, Krakow 2004.

Nye jr. J.S., *Soft Power. Jak osiągnąć sukces w polityce światowej*, Warszawa 2007.

Pawłowski J., *Broń masowego rażenia orężem terroryzmu*, Warszawa 2004.

Pawłowski J., *System przeciwdziałania rozprzestrzenianiu broni masowego rażenia*, Warszawa 2008.

Pietrzak W.B., *Terror atomowy – czy tylko kwestia czasu?*, "Raport – Wojsko Technika Obronność' 2004, No. 2.

The Davy Crockett, http://www.brookings.edu/projects/archive/nucweapons/davyc.aspx, (accessed 15.04.2012).

Witczak M., Kot B., *Ocena możliwości użycia broni masowego rażenia w przyszłych konfliktach zbrojnych i wynikające z niej zagrożenie dla terytorium Polski*, "Myśl Wojskowa" 2005, No. 6.

Zenko M., „*A Nuclear Site Is Breached" – South African Attack Should Sound Alarms, Belfer Centers for Science and International Affairs*, http://belfercenter.hks.harvard.edu/publication/17791/nuclear_site_is_breached.html, (accessed 29.10.2012).