ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ
SCIENTIFIC JOURNAL OF POLISH NAVAL ACADEMY

2016 (LVII) 1 (204)

DE GRUYTER

DOI: 10.5604/0860889X.1202431

Radosław Ambroziak*, Sławomir J. Ambroziak, Ryszard J. Katulski**, Jarosław Sadowski**, Jacek Stefański**, Edyta Lelo*****

BIOTERRORISM — CHARACTERISTICS AND POSSIBILITIES OF PREVENTION

ABSTRACT

In the paper bioterrorist threats have been presented. Historical background and possible methods of attacks have been described. The most dangerous pathogens and disease entities have been classified. Selected methods of detection and identification of biological weapon have been presented. The wireless system for threats monitoring — developed at Gdansk University of Technology — has been described.

Key words:
biological threats, bioterrorism, wireless system for threats monitoring.

INTRODUCTION

The more globalised the world becomes, the more threats for human lives appear. The threats are often independent of human activities, but there are numerous ones related to crime or terrorism. One of the most threatening is terrorism with the use of biological agents.

Bioterrorism is a phenomenon of illegal use of biological agents against a civilian population to influence the policy of a government in the pursuit of personal, political,

* Multinational Corps Northeast, Waleriana Łukasińskiego 33 Str., 71-215 Szczecin

** Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics, G. Narutowicza 11/12 Str., 80-233 Gdańsk, Poland; e-mail: {sj_ambroziak; jkat; jaroslaw. sadowski; jstef}@eti.pg.gda.pl

*** Alumnus of Nicolaus Copernicus University Collegium Medicum in Bydgoszcz, Jagiellońska Str. 13-15, 85-067 Bydgoszcz

religious or/and other goals [5, 6, 8, 16, 17]. It is worth noticing that research, production and stockpiling of biological and toxic weapons is forbidden both in Poland [9] and in the world [11].

This paper discusses threats related to bioterrorism, its historical overview in relation to initial use of biological weapon (weapon B) and possible methods of conducting bioterrorist attacks. The classification of the most dangerous pathogens and disease entities focuses on anthrax, plague and smallpox. Another section describes the methods of detecting and identifying biological weapons. The last chapter presents a wireless system for threats monitoring developed at the Department of Radio Communication Systems and Networks at Gdansk University of Technology. Due to the use of appropriate biosensors, that can make early detection of biological threats possible, the system significantly raises the security level.

HISTORICAL OVERVIEW

It is believed that the first recognized bioterrorism attack was during the siege of Caffa in 1346. The Tartars hurled the cadavers of their deceased into the city initiating a plague epidemic [2, 5, 16, 17]. In 1495 in Naples, the Spanish contaminated wine with the blood of lepers and gave it to the French. During the French-Indian war in 1767 in North America, sir Jeffrey Amherst distributed blankets contaminated with smallpox virus to native Americans supporting the French [2, 16, 17].

World War II and the post-war times was the period of intense research on biological weapon. The Japanese conducted research on anthrax over the period 1932–1945 [2, 5, 16] and Great Britain carried out independent research on anthrax bombs [2, 5, 16]. The USA started an offensive biological warfare program in the period of 1941–1943 and diseases of interests to this program were plague, cholera and Q-fever [2, 17]. Those extensive developed programs were run in the cold war period [2, 5, 16] and lasted until 1969 when the USA declared the end of their activities related to B weapons. However, although many countries signed BWC (*Biological and Toxin Weapon Convention*) in Geneva in 1972 [9, 11], an epidemic of anthrax occurred among the citizens of Sverdlovsk (Russia). It was 13 years later when they admitted that it started near the Soviet military microbiology laboratory. As a result, 96 people were infected and 64 of them died [5, 17].

One of the most spectacular bioterrorism attacks was in 1984 in Dallas, USA, caused by Rajneeshee's followers who poisoned food with *Salmonella Typhimurium*. Seven hundred fifty one people contracted *salmonellosis* as a result of the attack;

45 of them were hospitalized [2, 5, 16, 17]. In 1995 The Aum Shinrikyo attacked the Tokyo subway killing 12 people, severely injuring 50 and 5000 were hospitalized [2, 16]. The terrorists used sarin, the gas that paralyses nervous system. After 11/9 in 2001 in the USA, came the outbreak of anthrax caused by weaponized spores that were mailed through the postal system. Consequently, 22 people were infected, 5 died and over 32000 were treated with ciprofloxacin [2, 5, 17].

METHODS OF BIOTERRORISM

The knowledge of possible methods of bioterrorism is a very important factor for taking up counteractions and helping lessen the destructive effects [17]. There are a few methods of bioterrorism. The first having the most dangerous consequences is an aerosol attack. Contamination of air is a special threat that is difficult to detect and may lead to multiple fatalities [4, 14, 17]. Another threat is water or/and food intoxication [4, 5, 14, 17], which can result in an outbreak of a severe epidemic [5, 14, 17]. According to the Polish Ministry of National Defence the most possible bioterrorist attack in Poland can be food intoxication [14]. There are also some unconventional methods such as: transmitting pathogens through postal system [4, 14, 17], carrying loads with biological weapons in cargo containers [17] or agro terrorism [11]. An unconventional attack is difficult to detect due to the variety of existing methods and difficulties in predicting attackers future actions [17].

CLASSIFICATION OF PATHOGENS AND DISEASE ENTITIES

According to *American Centres for Disease Control and Prevention* (CDC) pathogens can be categorized according to the level of threat they represent:

- category A — these high-priority agents pose a risk to national security, can be easily transmitted and disseminated, result in high mortality, have potential major public health impact;
- category B — these agents are moderately easy to disseminate and have lower morbidity and mortality rates than agents of A group;
- category C — these agents are emerging pathogens that might be engineered for mass dissemination because of their availability, morbidity and high mortality rate.

There are some very dangerous disease entities related to the above mentioned pathogens, i.e.:

- anthrax — caused by the bacteria *Bacillus anthracis* [9, 13], a leading agent on the list of potential biological weapons [3], mortality rate among untreated patient can be 20–97%;
- pestis — caused by the bacteria *Yersinia pestis* — mortality rate among untreated patient can reach 20 up to 100%;
- smallpox (*Variola vera*) — caused by the virus *Variola major* [2, 17] — mortality rate can be about 30% [2];
- viral hemorrhagic fevers (VHFs) — caused by RNA viruses *Flaviviridae, Bunyaviridae, Arenaviridae and Filoviridae* [10] — mortality rate can be about 10–15% (for Ebola and Marburg even 50–90%).

METHODS OF DETECTING AND IDENTIFYING BIOLOGICAL THREATS

There are already known technologies that make detection of an aerosol threat possible, even from a great distance. One example of such a solution is *A Long Range Biological Standoff System* (LRBSDS) that can detect an aerosol cloud from the distance of 30 km. This system consists of a laser transmitter, a receiver and telescope. Another solution is The Joint Biological Standoff Detection System (JBSDS) that can monitor a detected aerosol cloud. *The Interim Biological Agent Detection System* (IBADS) [1, 12] is a semiautomatic system with an aerosol concentrator and aerodynamic particle sizer. *The Joint Portal Shields* (JPS) is the first highly automated system that is monitored by a central computer identifying 8 biological factors within 25 minutes. *The Joint Biological Point Detection System* (JBPDS), the next system of this kind, can detect 10 agents within 20 minutes. One of the portable devices is *The Joint Biological Agent Identification and Diagnostic System* (JBAIDS), that is developed for identifying both environmental and clinical samples [12]. *Fluorescence Aerodynamic Particle Sizer* (FLAPS) is another highly advanced system that is able to distinguish between biological particles and inanimate material [1, 12]. The prototype system *Light Detection and Ranging* (LIDAR) [15, 17], whose co-authors are Polish scientists from the Institute of Optoelectronics of The Military University of Technology [15], can detect aerosol particles in the distance of 100 kilometres [3].

Biosensor techniques can detect bio aerosols or allow to identify biological agents [12].When searching for specific antigens, these techniques usually use optical fibre with encapsulated antibodies. Antibodies bound to the searched antigen are

detected with antibody marked with fluorescent agent. The laser light induces a signal that is registered by the detector. It facilitates marking in 'dirty samples'. This concept became a base for ANALYTE 2000 system (*Research International*) that can identify four samples at the same time using four probes. This instrument provides sensitivities to 3–30 biochemical agents within 20 minutes. RAPTOR (*Research International*) is even more sensitive, and its identification time is shorter [1, 12]. *The Ruggedized Advanced Pathogen Identification Device* (RAPID) as a portable automated real-time PCR system designed to identify biological agents [1, 12] became a ground-breaking device. Because of its reliability and accuracy it is the ideal choice for the army, mobile analytical labs and field hospitals [12].

Luminometry is a method of ATP detection (adenosine 5'-triphosphate) in living cells by detecting light emitted during enzyme decomposition of ATP. The emitted energy is proportional to ATP content in a sample and can be marked with a photodetector — luminometer [1, 15]. Luminometric technique can be applied for an immediate detection of bacteria in liquids, powders and lyophilises [1]. It also helps to investigate contaminated surfaces, food, water, air and detect bacterial spores in examined samples. One of few systems used for measuring ATP content is PROFILE system that can distinguish eukaryotic cells from prokaryotic ones [1, 15]. It is worth noting that there are some portable field diagnostic tests (*rapid diagnostic tests*) also called HHA (*Hand-Held Assay*) that are used for initial diagnosis under field conditions, i.e: Alexeter Technology for detection and identification of a single biological agent or Advent Biotechnologies for detection of a few agents.

WIRELESS SYSTEM OF THREATS MONITORING

Threats monitoring has numerous applications in many aspects of human life in the XXI century, and became an important issue for national and regional authorities responsible for public security. Various data are subject to acquisition and control. These data are related with the transport (both land and marine), parameters of industrial processes, as well as degree of atmospheric pollution. It is also important to usage of monitoring systems in minimizing risks of terror acts, including bioterrorism. In connection with foregoing, there is a need for new solutions of data monitoring network. Applying a concept of wireless system of threats monitoring allows to increase efficiency and reliability of monitoring systems.

This issue became a subject of research at the Department of Radio Communication Systems and Networks at the Gdansk University of Technology, where the original concept of the data monitoring system with self-organizing sensors network

was developed. This network allows for monitoring of various threats of public security [7], including bioterrorism.

The self-organizing network of multipurpose data transfer nodes (MDTN) is a basic part of the monitoring system (fig. 1). Each of these nodes can be equipped with various wireless interfaces, depending on the intended use of a particular solution. For wireless communication with radio access core network following radio interfaces can be used: GSM, UMTS, LTE, TETRA, WiMAX or Inmarsat. Multipurpose data transfer nodes are communicating with each other via short-range wireless interfaces, such as Bluetooth, ZigBee or WiFi.

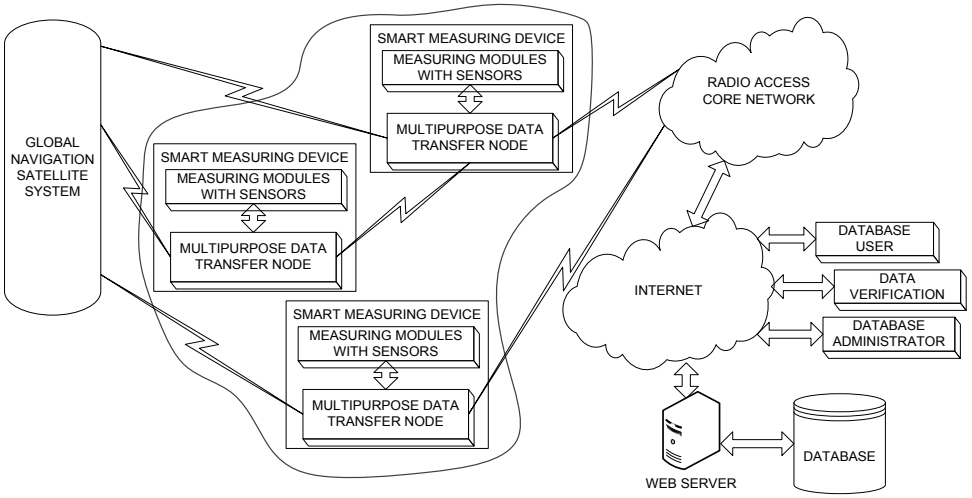

Fig. 1. Block diagram of the Wireless System for Threats Monitoring

A separate issue is the GNSS (Global Navigation Satellite System) receiver, whose presence in MDTN depends on whether the system requires localization of measurement or not. It may be the GPS receiver, and in the future it may be the receiver of GLONASS or GALILEO. MDTN may also be equipped with a number of wire interfaces (USB, RS232, RS485, Ethernet), e.g. enabling connectivity with the measuring modules, change configuration of MDTN, etc.

Each MDTN is connected to the measurement modules, creating the smart monitoring device (SMD) that is responsible for receiving, collecting and sending data from sensors and GNSS receiver. Set of monitored parameters closely depends on the particular application of monitoring system. In the considered case the SMD may include measurement solutions described in previous section of the paper, in particular biosensors. There is a large flexibility in configuration of sensor network. It is limited only by availability of sensors for particular parameters.

The SMDs (being powered by batteries) in wireless sensor networks should be able to unmanned work, what implies very low power consumption without losing their functionality. Apart from direct communication with the radio access core network, SMD is able to connect to that network in an indirect way, by organizing with others SMD modules at ad-hoc network. In this way, reliability and efficiency of data monitoring system are increased. The measurement data are sent to the database located on web server through the radio access core network, further through the Internet. In order to avoid incorrect entries or false alarms, measurement data are verified before writing to the database. Access to data is possible via the Internet, both for users and for system administrators.

CONCLUSIONS

This paper discusses threats related to bioterrorism, its historical overview in relation to initial use of weapon B and possible methods of bioterrorist attacks. The classification of the most dangerous pathogens and disease entities focuses on anthrax, plague and smallpox. This paper describes the methods of detecting and identifying biological weapons, and presents a wireless system for threats monitoring developed at Gdansk University of Technology. Due to the use of appropriate biosensors, that can make early detection of biological threats possible, the system significantly raises the security level.

REFERENCES

[1] Bartosze M., *Metody wykrywania zagrożeń bronią biologiczną*, 'Przegląd Epidemiologiczny', 2003, No. 57, pp. 69–76 [*Methods used to detect biological weapon threats* — available in Polish].

[2] Binczycka-Anholer M., Imiołek A., *Bioterroryzm jako jedna z form współczesnego terroryzmu* [*Bioterrorism as a form of modern terrorism*], [bilingual], 'Hygeia Public Health', 2011, No. 46(3), pp. 326–333.

[3] Chomiczewski K., *Patogeny zwierzęce jako broń biologiczna*, 'Przegląd Epidemiologiczny', 2003, No. 57, s. 55–61 [*Animal pathogens as a biological weapon* — available in Polish].

[4] Chomiczewski K., *Zagrożenie bioterroryzmem*, 'Przegląd Epidemiologiczny', 2003, No. 57, pp. 349–353 [*Bioterrorist threat* — available in Polish].

[5] Czuba K. et al., *Bioterroryzm — zagrożenie, zasady postępowania, regulacje prawne*, 'Biuletyn Wydziału Farmacji WUM', 2011, No. 2, pp. 28-33 [*Bioterrorism — threat, emergency preparedness, law regulations* — available in Polish].

[6] Daniszewski P., *Bioterroryzm — zagrożeniem dla bezpieczeństwa regionalnego i światowego*, 'International Letters of Social and Humanistic Sciences', 2013, No. 1, pp. 28–34 [*Bioterrorism — threat to regional and world security* — available in Polish].

[7] Katulski R., Namieśnik J., Stefański J., Sadowski J., Wardencki W., Ambroziak S. J., *Wireless systems of threats monitoring*, IEEE International Conference on Technologies for Homeland Security, Boston 2010.

[8] Kępka P., *Bioterroryzm. Polska wobec użycia broni biologicznej*, Difin, Warszawa 2009 [*Bioterrorism. Poland and use of biological weapons* — available in Polish].

[9] *Konwencja o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu, sporządzona w Moskwie, Londynie i Waszyngtonie dnia 10 kwietnia 1972 r.*, Dz.U. 1976, No. 1, Pos. 1 [*The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction opened for signature on 10 April 1972 in Moscow, London and Washington*].

[10] Korzeniowski K., *Wirusowe gorączki krwotoczne*, 'Forum Medycyny Rodzinnej', 2012, Vol. 6, No. 5, pp. 205–221 [*Viral hemorrhagic fever* — available in Polish].

[11] *Seventh Review Conference of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction*, Geneva 2012.

[12] Szopa M., Pędlowski M., Szulc J., Futoma-Kołoch B., *Szybkie testy diagnostyczne na polu walki*, 'Laboratorium', 2014, No. 3–4, pp. 28–31 [*Fast diagnostics tests in the battlefield* — available in Polish].

[13] Zajkowska J., Hermanowska-Szpakowicz T., *Wąglik jako broń biologiczna*, 'Medycyna Pracy', 2002, No. 53(2), pp. 67–72 [*Anthrax as biological weapon* — available in Polish].

[14] http://www.antyterroryzm.republika.pl/raporty_csips.pdf, [access 10.03.2015].

[15] http://www.cresz.wp.mil.pl/plik/file/EpiMilitaris2013/Materialy_konferencyjne/Chomiczewski_pol_ang.pdf, [access 28.02.2015].

[16] http://www.laboratoria.net/home/13198.html, [access 01.03.2015].

[17] http://www.sprzet-ratowniczy.pl/files/attachments/news/4f740fb9-BIOTERRORYZM.pdf, [access 10.03.2015].

ZAGROŻENIA BIOTERRORYSTYCZNE — CHARAKTERYSTYKA ORAZ MOŻLIWOŚCI PRZECIWDZIAŁANIA

STRESZCZENIE

W artykule przedstawiono zagrożenia związane z bioterroryzmem. Zaprezentowano rys historyczny oraz opisano możliwe drogi przeprowadzania takich ataków. Sklasyfikowano najgroźniejsze patogeny i zaprezentowano najniebezpieczniejsze jednostki chorobowe. Przedstawiono wybrane metody detekcji i identyfikacji zagrożeń bronią biologiczną. Zaprezentowano opracowany na Politechnice Gdańskiej system bezprzewodowego monitoringu zagrożeń bezpieczeństwa, który może wpłynąć na poziom bezpieczeństwa poprzez wczesne wykrywanie zagrożeń biologicznych.

Słowa kluczowe:

zagrożenia biologiczne, bioterroryzm, bezprzewodowy monitoring zagrożeń.