

Michał Stępiński

## **1. FORMAL AND LEGAL BASIS FOR COMBATING TERRORISM**

The threat of the use of CBRN-E in terrorist attacks means that law enforcement agencies must always be prepared to respond to such threats. This is just one part of the fight against terrorism. Efficiency in under such conditions requires interdisciplinary knowledge of:

- The formal and legal basis for combating terrorism;
- Decision-making under emergency conditions (e.g. in terrorist attacks);
- Terrorism as a threat to public order;
- Anti-terrorist actions involving CBRN materials.

Knowledge of these areas will help incident responders to identify the threats posed by terrorism to public safety, to understand the functioning of the various anti-terrorist systems, and to prepare them for decision-making in response to terrorist incidents – particularly CBRN-E.

Ensuring public security is one of the basic functions of the modern state. Terrorism is one of the greatest threats to the world and forces us to take action in the fight against it, to prevent and react to attacks. Like any state activity, the fight against terrorism must be based on legally binding acts and organisational arrangements. These must be influenced by both the domestic and international environments. Escalation of the potential for terrorist threats makes it necessary to continually improve anti-terrorism systems. Understanding the formal and legal bases for combating terrorism, and knowing what the legal and public security procedures are at the site of a terrorist attack, are all necessary preparations in the fight against terrorism. Security specialists should:

1. Have a basic knowledge of the structures and institutions of the state, including in the field of Counter-terrorism (CT), and the relationships between them.
2. Have an elementary knowledge of the international security structures, institutions and organisations combating terrorism in the EU, and the relationships between them.
3. Be able to utilise basic theoretical knowledge to analyse specific processes and social phenomena, and characterise the national security environment, including its dynamics and essential elements of the fight against terrorism.
4. Be able to analyse the causes and course of specific processes and phenomena in the field of international security. This provides the specialist with

a knowledge and understanding of the mechanisms of the various institutions, especially those engaged in combating terrorism.

5. Be able to participate in the preparation of various CT activities in national and international security, taking into account the legal and political aspects.

### **1.1. Basic concepts of counter-terrorism**

State reactions to terrorist threats should consist in a complete, coherent system that provides for the most effective operations. The most common model includes activities in two areas:

1. Combating terrorism through society as a whole (defensive actions).
2. Combating terrorists directly (offensive actions).

This division takes into account NATO's military concept of defence against terrorism, which defines the fight against terrorism as the preventive, defensive and offensive measures taken to reduce the vulnerability of forces, individuals and property to terrorist threats and acts of terror. In the context of the NATO Comprehensive Approach, this can be combined with or followed by measures enabling recovery from terrorist acts. This position indicates that, despite NATO's military character, it takes a broader view of security into account. NATO activities in this area focus on:

- Compliance with International Law;
- Support for Allies;
- Non-Duplication and Complementarity.

NATO's international CT work is achieved through, amongst others, close contact and ongoing communication with various international organisations, including the United Nations, the European Union, the Organization for Security and Co-operation in Europe (OSCE), and the Global Counterterrorism Forum (GCTF). An example of its engagement in Europe is the creation on February the 16<sup>th</sup>, 2017 of its Regional Hub for the South, based at NATO's Joint Force Command in Naples. The Hub is a focal point for enhancing both the Alliance's understanding of the challenges of the region and its ability to respond to them.

Proponents of the security sciences propose a number of different models for combating terrorism, analysis of which should provide a comprehensive approach to the issue. Some of these go beyond the scope of defensive and offensive activities.

Prevention of terrorism includes deterrents designed to discourage individuals or groups from engaging in terrorist activities, as well as the social policy of the state on people considered vulnerable to indoctrination by extremist groups. Combating terrorism has the following phases:

- Establish: recognize and identify opponents;
- Neutralise: arrest or eliminate threats;

- Punish;
- Impede: prevent opponents from returning to terrorist activity.

These phases include forecasting the identification of potential targets, risk analysis, and risk assessment of the likelihood of attacks. Responses include measures to minimise the effects of terrorist attacks. Protection should be provided for both people and infrastructure likely to be threatened by terrorists.

The most common model of combatting terrorism, however, is a model that consists of two phases:

1. Anti-terrorism.
2. Counter-terrorism.

### **1.1.1. Anti-terrorism**

Anti-terrorism is the combating of terrorism. K. Jałoszyński defines anti-terrorism as the use of protective measures reducing the vulnerability of people, forces and property to terrorism. It is realised in the following ways:

- Diplomatic;
- Economic;
- Administrative;
- Legal;
- Police and paramilitary;
- Intelligence;
- Social Policy.

**Diplomatic** activities involved in anti-terrorism are all forms of international policy aimed at creating a unified front against terrorism. The most visible manifestation of this is the formation of international anti-terrorist coalitions, which includes work between militaries or police forces. Poland is consistently present in the global anti-terrorist coalition.

**Economic** activities are focused on creating the capacity to control the flow of certain funds, to halt terrorist financing. For example, the US Patriot Act gave federal agencies the opportunity to request access to information from American financial institutions. This privilege has been strengthened with a tool for enforcing these demands. Refusal now results in an order to cease cooperation with any suspect entities. Within the Council of Europe, work in this area is primarily carried out by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL. This is a permanent monitoring body of the Council of Europe, entrusted with assessing compliance with principal international standards countering money laundering and the financing of terrorism, and monitoring the effectiveness of their implementation. It also has the task of making recommendations to national authorities on necessary improvements to their own systems. Through a dynamic process of mutual evaluation, peer review and regular follow-ups on

its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively. In Poland, the Chief Inspector of Financial Information is responsible for obtaining, collecting, processing and analysing information and taking action to counter money laundering and terrorist financing.

**Administrative** activities are aimed at the creation and improvement of government crisis response systems, which define the responsibilities of responders in taking concrete action to prepare for, react to, and recover from terrorist activities. One examples of this is the uniform system of alarm levels in the event of terrorist threats. Declaring an alarm imposes the obligation to perform the specific actions assigned to the given alarm level. This makes it possible to co-ordinate readiness to respond to terrorist events. These actions also include the issuing of decisions by the authorities, such as the prohibition of assembly in an area where there is a threat of a terrorist attack.

**Legal** activities consist in the creation of national and international law enabling prosecution and counter terrorism. Poland has ratified a number of international conventions and international agreements on the fight against terrorism, including those created by, for example:

- The United Nations;
- The Council of Europe.

These agreements, conventions, and decisions affect the international environment to varying degrees, and have different effects. One of the effects of international law is the cataloguing of crimes that cannot be considered political offenses that are nevertheless involved in a political offense, or committed for political reasons. The consequences of defining such a catalogue of crimes is to set aside the possibility of refusing to release the perpetrator of a terrorist offense to a state applying for extradition (the European Convention on the Suppression of Terrorism, Strasbourg, 27 January 1977). Another legal area in which anti-terrorist functions are being implemented is criminal law. Criminalization of terrorist behaviour is an essential element in the fight against terrorism. The Polish Penal Code defines terrorist offenses in Art. 115 Par. 20, making them a prohibited act punishable by imprisonment of at least 5 years. This includes the act of, or threatening to:

1. Seriously intimidate many people.
2. Force the authorities of the Republic of Poland or another state or organ of an international organization to take or discontinue certain activities.
3. Cause serious disturbances in the political system or economy of the Republic of Poland, other states or international organization.

Apart from terrorist crimes in Poland, the following are also related, punishable offenses:

- Leadership or participation in a group for the purpose of committing terrorist offenses;

- Financing of terrorism;
- Provision of knowledge and information for the purposes of committing a terrorist offense;
- Participation in training that would allow the commissioning of a terrorist offense;
- Crossing the border of the Republic of Poland to commit terrorist offenses in other countries;
- Making public calls for terrorist offenses;
- Persuading others to commit terrorist offenses (recruitment);
- Not sharing knowledge of planned terrorist offenses with the authorities.

**Police and paramilitary** activities are aimed at increasing police powers to stop people, check luggage and search residences; increasing security measures in public places that may be subject to terrorist attacks, and checking and strengthening critical infrastructure security. In these activities, the armed forces are often used as support for preventive and patrol activities in public spaces. An example of such a systemic approach is the VIGIPIRATE program, in which street patrols are made by units of the French Armed Forces.

**Intelligence** consists in gathering information and data basing it to enable the identification of suspects and the fight against terrorism. For these purposes, methods include the work of human agents, technical information gathering (eavesdropping, surveillance, satellite intelligence, etc), trawling the Internet, and so on. These activities are dealt with by special services with legal and technical capacities in these fields.

**Social policy** consists in running social programs discouraging terrorist activity, by counteracting radicalization, xenophobia and social exclusion. Successfully educating the public and residents of a country can limit the impact of terrorism on its society, and prevent it from developing in the first place.

### 1.1.2. Counter-terrorism

Counter-terrorism activities are carried out by special units that directly address the threat posed by terrorists using both firearms and non-lethal weapons. Counter-terrorism activities can be separated into:

- Counter-terrorist liquidation operations – conducted in response to terrorist incidents (combat rescue operations);
- Pre-emptive counter-terrorist combat actions – to prevent terrorist offenses by eliminating or stopping the perpetrators before they can act.

**Counter-terrorist liquidation operations** (combat rescue operations) are carried out by police or military units specialising in CT operations, with the aim of:

- Saving the lives of people threatened by terrorists;
- Neutralizing terrorists.

Characteristics of counter-terrorist liquidation operations include:

- Strict time limits;
- Immediate response;
- Highly dynamic action;
- Very high risk;
- Persistent threat to the lives and health of victims and CT operators.

Examples of counter-terrorist liquidation operations include the GIGN action against the Kouachi brothers in Dammartin-en-Goële, after the attack on Charlie Hebdo; the RAID action against Amedy Coulibaly at a kosher supermarket in Paris on the 10<sup>th</sup> of January 2015, and the BRI and RAID response in Paris, on the 13<sup>th</sup> of November 2015, in response to the attack at the Bataclan theatre.

**Pre-emptive counter-terrorist combat actions** are carried out by police or military units specialising in CT operations against terrorists who have been found to be still in the planning and preparation phase of their attacks, in order to:

- Stop or neutralise the terrorists;
- Prevent planned attacks from occurring.

Characteristics of pre-emptive counter-terrorist combat actions include:

- Time and place of the operation determined by the authorities/CT units;
- Detailed planning and preparation process;
- Highly dynamic implementation;
- Operations conducted so as to minimise the risk to civilians;
- Direct threat to the lives and health of the CT operators.

Examples of pre-emptive counter-terrorist combat actions include the January 15<sup>th</sup> 2015 arrest in Verviers, Belgium, of three Islamic terrorists at their place of residence (two were killed, one was wounded). The operation was carried out by the Belgian police's counter-terrorism unit (DSU), in a joint operation with the GIGN. In the same operation, 13 other terrorists were arrested.

Counter-terrorism tactics evolve with the methods and tactics of the terrorists. CT operators modify their tactics depending on the situation, as well as their equipment loadouts. All of their options are analysed to try to reach the ideal solution. In most countries, there are special rules for CT operators' use of firearms against terrorists (e.g. 'kill shots' and 'Shoot on sight/Shoot to kill'). This ground-level approach to fighting terrorism is particularly important to the safety and security of civilians.

## **1.2. Example: Combating terrorism in the Polish Republic**

Poland's anti-terrorist system is composed of services and institutions designed to identify and neutralise terrorist threats. It has appropriate powers and competences, is equipped with the means of providing a physical response,

and integrates communications systems, information exchange and direct action under the same command, all while keeping the public informed about real and potential threats. The Polish anti-terrorist system operates on three levels:

- Strategic;
- Operational;
- Tactical.

At the **strategic** level of the Polish anti-terrorist system, the legislation, anti-terrorism policy and organisational solutions needed to legally conduct CT operations are all devised. Systemic solutions are created at this level, defining the state's reactions in the event of terrorist incidents. Entities in the executive branch are supported by collegiate bodies, which provide substantive support in the implementation of the country's anti-terrorism operations.

The Prime Minister instigates activities by issuing regulations and guidelines for the implementation of statutory instruments in anti-terrorism policy. He also works directly, overseeing the work of the Government Crisis Management Team.

The Council of Ministers is then responsible for establishing and approving counter-terrorism strategy, subsequently creating state policy around it. It also makes decisions on other applicable regulations. The Council can also ask the president to declare a state of emergency, and pass emergency laws. To assist the Council of Ministers in its work, the Interdepartmental Task Force on Terrorist Threats was established, which is chaired by the Minister of Internal Affairs.

The Minister of Internal Affairs is responsible for the protection of public security and public order, and for crisis management. In emergency situations, it can work independently. The Minister is also responsible for the preparation, response and re-supply of the resources used to combat terrorism. The Minister of Internal Affairs supervises the services working in the anti-terrorist system, including the Police, Border Guard, Government Protection Bureau, and Fire Department.

The Interdepartmental Task Force on Terrorist Threats is an auxiliary body of the Council of Ministers, and is appointed by the Prime Minister. Its meetings are held on a regular basis, as and when needed. The Task Force consists of:

- Chairman – Minister of Internal Affairs;
- Deputy – Minister in charge of public finance, Minister of National Defence, Minister of foreign affairs, Minister of Justice, and Members of the Council of Ministers, Coordinator of Special Services;
- Secretary – a person appointed by the chairman of the team from the staff of the office, to serve the Minister of Internal Affairs;
- Secretary of State at the Ministry of Interior;
- The Secretary of the Special Services Board, or their substitute;
- Chief of Civil Defence of the country or their deputy;
- The Head of the Internal Security Agency or their deputy;

- The Head of the Foreign Intelligence Agency or their deputy;
- The Head of the Government Protection Bureau or their deputy;
- Commander in Chief of the Police or their deputy;
- Commander in Chief of Border Guards or their deputy;
- Commander in Chief of the State Fire Service or their deputy;
- The Chief of General Staff of the Polish Army or their deputy;
- Operation Commander of the Armed Forces or their deputy;
- The Head of the Military Intelligence Service or their deputy;
- The Head of the Military Counterintelligence Service or their deputy;
- Commander in Chief of the Military Police or their deputy;
- General Inspector of Revenue Control or its replacement;
- General Inspector of Financial Information or their replacement;
- Head of the Customs Service or their deputy.

The Interdepartmental Task Force on Terrorist Threats' responsibilities include:

- Monitoring, analysis and evaluation of terrorist threats;
- Presentation of opinions and proposals to the Council of Ministers;
- Development of draft anti-terrorism standards and procedures, in particular standards for assessing and evaluating the presence of a threat;
- Initiation, coordination and monitoring of activities undertaken by the competent governmental administration, particularly regarding the use of information and the identification, counteracting and combating of terrorism;
- Requesting the appropriate ministers to take legislative action to improve the means and forms of combating terrorism;
- Arranging work with other countries in the fight against terrorism and coordination of the exchange of information and joint operations;
- Initiating training sessions and conferences on counter-terrorism.

Finally, the Government Crisis Management Team is the body responsible for initiating and coordinating crisis management activities, including those related to terrorist threats. It is the task of the Team to prepare proposals for the use of forces and resources needed to deal with emergencies, and to advise on the coordination of the activities of governmental authorities, including in the case of terrorist attacks.

The **operational** level of Poland's anti-terrorist system handles the coordination of information exchange and work between anti-terrorist system operators, including the ongoing analysis of terrorist threats. The Internal Security Agency's Anti-Terrorism Centre is responsible for coordinating analytical and information activities conducted by all anti-terrorist organizations.

The essence of the Centre's activity is the rapid and efficient transmission of information on terrorist threats, specifically:

- Terrorist incidents occurring outside the Republic of Poland that affect the security of Poland and its citizens;

- Terrorist incidents occurring inside the Republic of Poland that affect the security of Poland and its citizens;
- Information on potential threats to Poland and abroad;
- Information on money laundering or transfers of funds that may indicate the financing of terrorist activity.

The Anti-Terrorism Centre is active all the time, and is staffed by officers and soldiers who provide all of its services as part of the country's AT system.

The Government Security Centre/Government Crisis Management Team fulfils the role of a national crisis management centre. It provides full-time, on-call duty for crisis management issues, permanent on-call defence forces, and exchange of information on international and national issues, including implementation of the NATO Crisis Response System.

The **tactical** level of the anti-terrorist system encompasses ground-level combat forces and emergency responders involved in the protection of Poland. These include:

- Internal Security Agency;
- Foreign Intelligence Agency;
- Military Counterintelligence Service;
- Military Intelligence Service;
- Central Anti-Corruption Bureau;
- General Inspector of Financial Information;
- Police;
- Border Guard;
- Government Protection Bureau;
- Fire Brigade;
- Customs Service;
- Military Police;
- Ministry of National Defence;
- Ministry of Foreign Affairs.

All of these entities carry out the tasks resulting from the legal provisions directly connected with prevention, preparation for reacting, reacting and rebuilding of resources after activities conducted within the anti-terrorist system of the Republic of Poland.

### **1.3. The legal basis for combating terrorism**

Over the last few years, the legal and organisational framework for combating terrorism in Poland has changed significantly:

- Until 2014, there were no systemic regulations;
- In 2015–2016, attempts were made to streamline operations at the political and administrative levels;

– 2016 saw the introduction of the Act of 10 June 2016 on Counter-terrorism Activities. This comprehensive law regulates the fight against terrorism at all levels.

Until as recently as 2014, the fight against terrorism in Poland was based on a variety of scattered legal grounds, with many areas not regulated at all. Recognition, detection and prevention of terrorist offenses, and the prosecution of their perpetrators, were the domain of the Internal Security Agency. In this work, the ISA was the only one with any clearly indicated responsibility. Furthermore, there was no one service assigned the task of directly combating terrorism and responding to terrorist attacks. The most developed CT system at the time existed with the Police, as part of their overall remit to protect public safety. Eventually, the lack of fully-fledged anti-terrorist law was seen to be very dangerous when it appeared that terrorist attacks could actually happen in Poland. Concerns were so great that in 2015 an administrative agreement was signed between the heads of the major emergency services, designating responsibility for terrorist incidents. The co-signees were the:

- Head of the Internal Security Agency;
- Commander in Chief of the Police;
- Commander in Chief of the Border Guard;
- Commander in Chief of the Military Police;
- Commander in Chief of the State Fire Service.

The agreement states that, in the event of terrorist incidents or suspicion of such incidents, incident management shall order the services' work together through appropriate utilisation of personal, material and financial resources. As a general rule, it was assumed that responding officers would be managed by a Police officer and a Military Police officer.

The next step taken in building responsibility for Poland's anti-terrorism response came in 2014, with the enactment of the 2015–2019 National Anti-terrorist Program. In the core document of the program, a general interpretation of the responsibilities of the various entities in Poland's anti-terrorist system was made, in the context of the legal framework. The National Anti-terrorist Program was not a source of legislation itself, and although it didn't alter the extent of the duties of the individual services involved, it did clarify them. It also crystallised the importance of the need for co-ordination of the activity of the participating services, and defined the range of duties of the heads of the services as at January 2015. The police are responsible for coordinating threat response in civilian areas, with the Military Police (with the consent of the subordinate parts of the Ministry of National Defence).

But the breakthrough moment for the gradually coalescing anti-terrorist system in the Republic of Poland came in 2016, when the Act of 10 June 2016 on Anti-terrorist Activities (Journal of Laws of 2016, item 904) was passed. It was originally created to ensure safety at the NATO summit in Warsaw and the

World Youth Day in Krakow, both in July of that year. The Act comprehensively regulates the fight against terrorism in Poland, and specifies which entities have which duties. Some of its stipulations sanction the existing organisational arrangements, and also legally oblige the various services to perform certain tasks. The Act also introduced special rules on the use of weapons in counter-terrorist operations.

#### **1.4. Example: The 2015–2019 National Anti-Terrorism Program**

Adopted by the Council of Ministers in 2014, the main objective of the 2015–2019 National Anti-terrorist Program was to legally reinforce and clarify Poland's anti-terrorist system. With this in mind, the Program sets specific objectives:

- Improve the nation's capacity to prevent terrorist attacks;
- Strengthen the preparedness of services and institutions for the possibility of terrorist incidents;
  - Increase responsiveness in the event of a terrorist incident;
  - Improve the efficiency of the forces and resources utilised;
  - Improve existing procedures for dealing with terrorist threats.

These objectives are met in order to better respond to, and deal with, the following events, which are classified as being terrorist incidents:

- Detonation of explosive devices;
- Assault with firearms;
- Abduction of people, including taking them abroad;
- Occupation of means of transport, including the holding of hostages;
- Abduction of means of transport:
  - land transport,
  - water transport,
  - air transport.
- Assault with aircraft having RENEGADE status;
- Assault with a vessel or a floating object for which it was granted the status of MARITIME RENEGADE;
- Assault on the health, life or freedom of protected persons;
- Assault with the use of:
  - Biological agents,
  - Chemicals,
  - Radioactive material.
- Cyber terrorist attacks;
- Attacks on critical infrastructure;
- Other types of terrorist attack;
- False notification of a terrorist threat.

For each of the five specific objectives listed above, areas of responsibility were identified and priorities assigned in the various phases of anti-terrorism prevention and response in Poland, as well as the lead entity in charge of each phase. These can be broken down as follows:

### **Prevention**

1. Recognising terrorist threats – Internal Security Agency (international terrorism is handled by the Foreign Intelligence Agency).
2. Analysing, forecasting and assessing terrorist threats, including conducting analytical and information-gathering activities – Internal Security Agency (international terrorism is handled by the Foreign Intelligence Agency).
3. Coordinating the exchange of information on terrorist threats – Internal Security Agency.
4. Monitoring the media for information with which to prevent terrorist incidents – Internal Security Agency.
5. International cooperation on the prevention of terrorist threats – Internal Security Agency.
6. Informing the public of terrorist threats – Internal Security Agency.
7. Counteracting the financing of terrorism – General Inspector of Financial Information.
8. Public information and education policy – Ministry of the Interior.
9. Migration and asylum policy – Ministry of the Interior.
10. Protection of the state border – Border Guard.
11. Protection of Polish airspace – Polish Armed Forces.
12. Participation in stabilization, peacekeeping and international missions, and anti-terrorist coalitions – Ministry of National Defence.

### **Preparedness**

Although the 2015–2019 National Anti-terrorist Program does not designate responsibilities in the preparedness phase, the following areas of action are identified:

1. Development of plans and increasing of resources.
2. Evaluation of potential targets of terrorist attack.
3. Critical Infrastructure Protection.
4. Protection of transport systems.
5. Protection of population centres.
6. Work with the private sector.
7. Participation in exercises and training.

## **Response**

In responding to a terrorist incident, the following areas of action are specified:

1. Oversight of crisis management on the territory of Poland – The Council of Ministers (in urgent situations – the Minister of Internal Affairs).
2. Oversight of the Government Crisis Management Team – The Prime Minister (in urgent situations – the Minister of Internal Affairs or the Minister of National Defence).
3. Provision of crisis management services to the Government Security Centre.
4. Coordination of information exchange and the information policy of the public administration during a crisis – Government Security Centre.
5. Preparation for launching emergency management procedures (in the event of an incident) – Government Security Centre.
6. Actions against floating facilities used in terrorist attacks – Border Guard, followed by the Polish Armed Forces.
7. Actions against aircraft used in terrorist attacks – the Polish Armed Forces.
8. Recovering personnel lost as a result of abduction by terrorist organizations or organized crime groups – Ministry of Foreign Affairs (for soldiers – Ministry of Defence).
9. Recommendations for handling crises as a result of terrorist incidents, that threaten critical infrastructure, the life or health of people, property of considerable size or national heritage, etc, or the environment – Internal Security Agency.
10. Creation, conduct and coordination of information policy – Ministry of Interior.
11. Response to chemical contamination incidents, including in the context of terrorist attacks – the State Fire Service.
12. Responding to the use of biological agents in terrorist attacks – Ministry of Interior, with the support of the Ministry of Health, the Ministry of the Environment and the Ministry of National Defence.
13. Oversight of the elimination of nuclear threats to the nation, including in the context of terrorist attacks – Minister of Internal Affairs, with the help of the President of the National Atomic Energy Agency.
14. Decontamination procedures – Voivode or competent territorial self-government unit.

## **At an incident scene**

1. Medical emergency operations at the scene of a terrorist incident – State Medical Rescue and National Rescue and Firefighting System (at sea – Marine Search and Rescue Service).

2. Physical combat against terrorists/counter-terrorism – Police (on military territory – Military Police).
3. Securing incident scenes – Police (on military territory – Military Police).
4. Mining-pyrotechnic activities at an incident scene – Police (on military territory – Military Police).
5. Coordination the work of the emergency services at the scene of a terrorist incident in a pre-accession stage investigation – Police (on military territory – Military Police).
6. Investigation of terrorist incidents – Public Prosecutor’s Office.
7. Detection of terrorist offenses and prosecution of their perpetrators – Internal Security Agency.
8. Preliminary decontamination activities – State Fire Brigade.

### **Reconstruction**

At this stage, all of the entities involved in an incident response are required to re-supply the resources they need to respond to future incidents. The Minister for Internal Affairs is responsible for overseeing this task.

An Action Plan is also part of the 2015–2019 National Anti-terrorist Program, which specifies the projects to be implemented in all phases. Implementation of these tasks is overseen by the Interdepartmental Task Force on Terrorist Hazards, on the basis of a timetable for the tasks’ completion by the various services, developed by the heads of the individual services.

### **Competences of CT entities in the Republic of Poland**

Under the 2016 Act on Anti-terrorist Activities, the key entities in Poland’s anti-terrorist system, their areas of responsibility and powers are all clearly defined, as follows:

Head of the Internal Security Agency

Area of responsibility:

- Prevention of terrorist incidents.

Powers:

- Collecting information on terrorist threats;
- Coordination of analytical and informational activities undertaken by other services in the field of terrorist threats;
- Issuing information and instructions to entities threatened by terrorist incidents, to prevent, remove or minimise the threat;
- Maintaining a database on people involved in terrorist activities;
- Immediately informing the President of the Republic of Poland, the

Prime Minister, the minister responsible for Internal Affairs, the Minister for National Defence, the Minister for Foreign Affairs, the Minister for the Special Services Coordinator of any information relevant to preventing terrorist incidents;

- Coordination of intelligence and reconnaissance activities in terrorist incidents;

- Issuing recommendations to special services and supporting entities on eliminating or minimising the threat of terrorism;

- Implicit management of non-RP citizens using operational techniques (correspondence control, eavesdropping);

- Access to state registers;

- Issuing Police recommendations on protection of specific facilities, in the face of terrorist incidents;

- Appointing coordinating staff in the event of a terrorist alert or CRP (cyber terrorism) alert.

The Minister of Internal Affairs (Minister of Internal Affairs and Administration)

Area of responsibility:

- Managing terrorist incident response through planned actions, responding to incidents as they occur, and maintaining needed resources.

Powers:

- In urgent situations, the introduction, changing and cancellation of alerts;

- Applying to the Minister of National Defence for use of the Armed Forces of the Republic of Poland in assisting the Police in the event of third- or fourth-level alerts (acc. to the 4-level alert system used in Poland);

- Supervising the Police, Border Guard, State Fire Service and Government Protection Office in their tasks under the Anti-Terrorism Act.

The Minister of Foreign Affairs (with the Minister of Special Services Coordinator)

Area of responsibility:

- Coordination of the activities of special services and entities responding to terrorist incidents outside the Republic of Poland, involving the citizens or property of the Republic of Poland.

Powers:

- Requesting appropriate departments and services to provide information, reports and options for proposed solutions;

- Requesting consultation on activities undertaken by special services and entities.

The Minister of National Defence (with the Minister of Foreign Affairs)

Area of responsibility:

– Coordination of the activities of special services and entities responding to terrorist incidents outside the Republic of Poland, involving the personnel or property of the Armed Forces of the Republic of Poland.

Powers:

– Requesting appropriate departments and services to provide information, reports and options for proposed solutions;  
 – Requesting consultation on activities undertaken by special services and entities.

Police/Military Police (In military areas)

Area of responsibility:

– Conducting counter-terrorist activities.

Powers:

– Directing anti-terrorist activities at the scene of a terrorist incident;  
 – Command of counter-terrorist forces.

### **1.5. System of police anti-terrorist units**

In February 1976, the first Polish counter-terrorist unit was established – the Security Department of the Capital of the Civic Militia, and was one of the first of its kind in Europe. The Germans had established their GSG-9 the year before, in 1974, while Austria formed its COBRA unit in 1977, the Portuguese their GOE in 1979, and France founded its RAID CT team in 1985.

Until 1990 in Poland, special militia forces were stationed in the largest regional towns, and these also had the task of combating terrorism. In 1990, specific Anti-Terrorism Units were then established in nine provincial capitals (Łódź, Gdańsk, Białystok, Rzeszów, Kraków, Katowice, Wrocław, Poznań, Szczecin), along with the Warsaw Police Department's own Anti-terrorist Department. In 2000, the name 'Anti-Terrorism Units' was changed to 'Independent Police Anti-terrorist Subdivisions'. At the same time, sub-units were created, being the Anti-Terrorist Sections of the Provincial Police Headquarters (in Opole, Gorzów Wielkopolski, Bydgoszcz, Olsztyn, Radom, Lublin and Kielce).

On March the 6<sup>th</sup>, 2003, the greatest tragedy in the history of Polish anti-terrorism occurred. The Warsaw Unit, which was at that time part of the Central Bureau of Investigation of the National Police Headquarters, stormed a house in which two dangerous criminals were hiding. As a result of the detonation of an explosive device, two policemen were killed and 17 wounded. During an exchange of gunfire, both the criminals were killed.

Over the next almost 15 years, until May 2017, the organizational structure of all Police Counterterrorism units was changed to make 18 independent anti-terrorist subdivisions stationed in all regional cities, with the Anti-terrorist Operations Bureau of the National Police Headquarters in Warsaw as the central, coordinating unit. At present, the Police have a system of counter-terrorist units prepared at all times to conduct combat activities throughout Poland, as well as to participate in joint operations in the EU.

### **1.5.1. The Anti-terrorist Operations Bureau at the National Police Headquarters**

The Anti-terrorist Operations Bureau at the National Police Headquarters [BOA KGP] is subordinate to the Deputy Commander of the Office of the National Chief of Police. The office is made up of combat units with specific specialisations, including a combat training division and a support division.

The BOA KGP's Tasks include combating terrorism and organising, coordinating and supervising the activities of the Police in this regard (counter-terrorist activities, including physical combat). In the execution of its tasks, it is legally considered a 'special intervention unit', as referred to in Council Decision 2008/617/JHA of 23 June 2008 on improving the cooperation between special intervention units of the Member States of the European Union in crisis situations.

The Commander in Chief of the Police, or the authorized Deputy Commander in Chief of the Police, direct the activities of the BOA KGP's officers within Poland. In the capital city of Warsaw and its surrounding Mazowieckie province, the Director of the BOA KGP directs the officers' activities.

### **1.5.2. The Independent Anti-Terrorist Sub-units**

These are subject to the Deputy Commissar of the Voivodship Police of the Department of Prevention, and consist of combat teams, a combat-training team, and a support team. Their tasks include:

- Preparation for and conduct of counter-terrorist activities, including physical combat;
- Preparation for and conduct of rescue operations in the event of direct threats to human life and health;
- Preparation for and conduct of combat operations requiring the use of specialized forces and means, or the application of special tactics;
- Implementation of tasks in the protection and support of protected persons;
- Conduct of pyrotechnic activities;
- Supporting rescue operations.

Conducting training and professional development of the police officers of the Police Counterterrorism Unit and the organisational unit of the Police Headquarters, competent in anti-terrorist matters, in terms of their acquisition of skills and competences and maintaining the high level of physical fitness necessary for the execution of their tasks. Their work is directed by the Voivodship Police Commander or an authorised deputy Voivodship Police Commander.

### **1.5.3. The Central Rear Guard Anti-Terrorist Unit of the Chief of Police**

The Police anti-terrorist units and the organizational unit of the Police Headquarters, which are competent in anti-terrorist matters, as well as mining and pyrotechnical units, constitute the Central Rear Guard Anti-Terrorist Unit of the Chief of Police (COAT KGP). Its tasks include:

- Actions requiring the use of the forces and resources of more than one anti-terrorism sub-unit of the Police, or its police mining and pyrotechnical units, carried out as part of police operations,
- Announcement of second-level emergency alerts (as described in the Decree of the Prime Minister on the list of projects and procedures of the crisis management system),
- Announcement of third-level emergency alerts (as described in the Decision of the Minister of Internal Affairs on establishing the manner and mode of introducing, changing or cancelling alert levels).

As soon as COAT KGP is activated, all Police AT units are subordinated to the COAT KGP commander. The COAT KGP commander could be the director or deputy director of BOA KGP, and is appointed each time by the Chief Police Officer. The COAT KGP commander has the authority to:

- Activate police anti-terrorist sub-units and police mining and pyrotechnical cells,
- Coordinate the use of the forces and resources of the anti-terrorist sub-units, and the police mining and pyrotechnical units,
- Recommend commanders for police operations to the commanders of counter-terrorism operations.

The Central Rear Guard Anti-Terrorist Unit of the Chief of Police is a driving force in the work of CT units throughout the country.

## **1.6. The ATLAS European Special Police Units network**

After the attacks in New York City on September 11, 2001, it seemed that nowhere in the world was secure, and that the threat of terrorism could take on an unprecedented scale. In the European Union, consideration was given

to strengthening its capacity to respond to terrorist threats. On October 15, 2001, in Brussels, at a meeting of 15 European police counter-terrorist units, the willingness to cooperate in the preparation of counter-terrorist operations was expressed. A slogan expressing this mutual desire was picked, *All Together To Protect You*. However, initial work on this mutual system of cooperation was undertaken without the support of the EU. In 2005, the Council of Europe adopted an anti-terrorism strategy. Then, in 2007, Javier Solana, the EU representative for Common Foreign and Security Policy, appointed Gilles de Kerchove as Counter-Terrorism Coordinator. The CT Coordinator was given the task of:

- Coordinating the work of the Council in the fight against terrorism;
- Presenting policy recommendations to the Council and propose action priorities, on the basis of threat analyses and reports prepared by the EU Intelligence Analysis Centre and Europol;
- Closely monitoring the implementation of EU Counter-Terrorism Strategy;
- Following all the instruments at the disposal of the European Union, regularly reporting to the Council and effectively implementing its decisions;
- Coordinating activities with the relevant preparatory bodies of the Council, the Commission and the EEAS, and sharing information about their work;
- Overseeing EU activity in the fight against terrorism;
- Improving relevant communications between the EU and other countries.

After this, in 2008 the legal basis for the operation and financing of the European ATLAS Collaboration Platform was established. This was made possible by the introduction of a number of Council decisions on cross-border cooperation and improved cooperation between the special intervention units of the Member States of the European Union. Chief among these was Council Decision 2008/617/JHA of 23 June 2008 on improving cooperation between the special intervention units of the Member States of the European Union in crisis situations (EU L 210, item 73). From the 1st of January 2009, it was then possible for special intervention units from one country to provide assistance to another European country, if requested, for assistance. This legal decision assumes that no one Member State has all of the means, resources and technical know-how needed to respond effectively to a crisis or crisis situation, requiring special intervention on a large scale. It was therefore considered essential that special intervention units meet on a regular basis and organise joint training sessions to share their experience. The records of these first meetings provided the opportunity for the ATLAS Group to act formally, and to obtain a budget from the Council of Europe. According to the ATLAS Convention, the aim of the group is to strive to create states in which every member of an anti-terrorist unit is at the same – highest possible – level. ATLAS achieves this by creating a network of mutual cooperation and assistance, thus achieving equal opportunities in the

fight against crime and terrorism (ATLAS Convention – not published). ATLAS members are national counter-terrorist units, as reported by their state authorities (limited to 2 units per member state). Units from non-EU countries can also be invited to participate as non-voting observers, after a majority vote by all voting members. These units are represented by their commander or a designated officer. ATLAS is managed by a president, elected for two-year terms (the current president is from COBRA, Austria), and this function is non-profit. Decisions are made jointly, at the ATLAS Commanders Forum twice a year. Organisational support is provided by the Executive Office, financed by the European Council, which gives ATLAS a budget of 1.5 million Euros. At present, ATLAS conducts training, information exchange, research projects and joint operations. Due to the situation in Europe, the cooperation of ATLAS units has become more important over the last two years, and today there are joint anti-terrorism operations all throughout the EU.

Since 2005, Poland's ATLAS member has been the Anti-Terrorist Operations Bureau of the National Police Headquarters. Units from Norway and Switzerland are included in ATLAS as observers, and in the event of a continued UK presence within the EU, SCO19 will also receive observer status. Altogether, ATLAS brings together 35 police CT units from 27 EU states:

1. ACVILA – Grupul Special de Protectie si Interventie 'Acvila' (The Eagle Unit), Romania.
2. AKS – Politiets Aktionsstyrke (The Special Intervention Unit), Denmark.
3. ARAS – Lietuvos policijos antiteroristinių operacijų rinktinė ARAS (Lithuanian Police Anti-terrorist Operations Unit ARAS), Lithuania.
4. ATJ Lučko – Antiteroristička jedinica Lučko (Anti-Terrorist Unit Lučko) Croatia.
5. ATU – Anti-Terrorism Unit, Switzerland.
6. BOA – Biuro Operacji Antyterrorystycznych Komendy Głównej Policji, Poland.
7. DELTA – Beredskapstroppen 'Delta' (The 'Delta' Emergency Response Unit), Norway.
8. DSI – Department of Special Interventions, Nederland.
9. DSU – The Directorate of special units (French: Direction des unités spéciales), Belgium.
10. EAO – Ειδικός Αντιτρομοκρατικός Ουλαμός (Special Anti-terrorist Squad), Cyprus.
11. EKAM – The Special Counter-Terrorist Unit (Greek: E.K.A.M. – Ειδική Κατασταλτική Αντιτρομοκρατική Μονάδα, Eidiki Katastaltiki Antitromokratiki Monada), Greece.
12. EKO Cobra – Einsatzkommando Cobra, Austria.
13. ERU – The Emergency Response Unit (Irish: Aonad Práinnfhreagartha), Ireland.

14. GEO – The Grupo Especial de Operaciones (Special Operations Group), Spain.
15. GIGN – Groupe d'intervention de la Gendarmerie nationale (National Gendarmerie Intervention Group), France.
16. GIS – Gruppo di Intervento Speciale (Special Intervention Group), Italy.
17. GOE – The Grupo de Operações Especiais (Portuguese for Special Operations Group), Portugal.
18. GSG 9 – Grenzschutzgruppe 9 der Bundespolizei (Border Protection Group 9 of the Federal Police), Germany.
19. KARHU – Karhu-ryhmä, The Police Rapid Response Unit (Finnish: Poliisin valmiusyksikkö), Finland.
20. K-Commando – K-Komando, Estonia.
21. LYNX – Útvar osobitného určenia Lynx Commando, Slovakia.
22. NI – Nationella insatsstyrkan, znana jako National Task Force of the Swedish Civilian Police (Swedish: Ordningspolisens nationella insatsstyrka), Sweden.
23. NOCS – The Nucleo Operativo Centrale di Sicurezza (Central Security Operations Service), Italy.
24. OMEGA – Pretterorisma Vieniba 'Omega' ('Omega' Counter-terrorism special police unit ), Latvia.
25. RAID – Recherche, Assistance, Intervention, Dissuasion (Search, Assistance, Intervention, Deterrence), France.
26. RED PANTHER – Specialna Enota Policije 'Red Panthers' ('Red Panthers' Special Police Unit ), Slovenia.
27. SCO19 – Specialist Crime and Operations Specialist Firearms Command, UK.
28. SEK BWL – Spezialeinsatzkommandos Baden-Württemberg (Special Deployment Commandos of the State of Baden-Württemberg), Germany.
29. SAG – Lo Special Assignments Group (Special Assignments Group), Malta.
30. SIAS – Serviciul Independent pentru Intervenții și Acțiuni Speciale (Independent Special Actions and Intervention Service, SIAS), Romania.
31. SOBT – Специализиран отряд за борба с тероризма – СОБТ (Special Unit for Combating Terrorism), Bulgaria.
32. TEK – Terrorelhárítási Központ (Counter Terrorism Centre ), Hungary.
33. UEI – Unidad Especial de Intervención (Special Intervention Unit), Spain.
34. URNA – Útvar rychlého nasazení – ÚRN (Rapid reaction unit), Czech Republic.
35. USP – Unité Spéciale de la Police (Special Unit of the Police), Luxembourg.

### **1.7. Grounds and procedures for working with foreign officers in anti-terrorist operations on Polish soil**

The European legal basis for joint responses to threats was created in 2008, with Council Decision 2008/615/JHA of 23 June 2008 on stepping up cross-border cooperation, particularly in the fight against terrorism and cross-border crime (Official Journal of the European Union 210 of 6 August 2008). This EC decision regulates the following areas:

- Conditions for and means of automatic transmission of DNA and fingerprint data;
- Conditions and procedures for transmitting other data on relevant international events;
- Conditions and procedures for providing information to prevent terrorist offenses;
- Conditions and procedures for intensifying cross-border police cooperation, including joint operations.

Among other things, it created the possibility of granting the powers of the host Member State officials under the direction and in the presence of a host Member State (including the use of firearms). The obligation to establish the details of a proposed joint operation was also established. Based on the EU law, Poland then passed the Act of 07 February 2014 on the participation of foreign officers or employees in joint operations or joint rescue operations in the territory of the Republic of Poland. This law regulates the mode and rules of participation of foreign officers in joint operations occurring on the territory of the Republic of Poland.

From Poland's perspective, joint operations are defined as actions conducted on its territory that involve foreign officers or employees of the Member States of the European Union, or other countries applying the Schengen acquis. These could be, for example:

- Joint patrols or other joint actions to protect public order, and for safety and crime prevention, carried out by officers or employees of the Police, Border Guard or Government Protection Bureau;
- In the case of assemblies, mass events or similar events, natural disasters and serious accidents, in order to protect public order and for safety and crime prevention, carried out by officers or employees of the Police, Border Guard or Government Protection Bureau;
- Within the framework of the assistance provided by the Special Intervention Unit referred to in Council Decision 2008/617/ HA of 23 June 2008 on improving the cooperation between the special intervention units of the Member States of the European Union in crisis situations, by police officers or employees of the Police, Border Guard or Government Protection Bureau.

To initiate a joint operation, the 'inviting' State must apply to a 'sending' State. Prerequisites for such invitations include:

- Explanation of the circumstances justifying a joint operation or joint rescue operation;
- An explanation of why, due to the nature of the incident justifying a joint operation or joint rescue operation, the use of only national forces and resources is impossible or insufficient;
- If a joint operation is agreed, in particular at a mass event or similar, a substantial number of nationals of the invited country are envisaged;
- By virtue of its nature, the participation of nationals of other States in an event justifying a joint operation, in particular a mass event or similar, can pose a serious threat to public security and order.

The persons qualified to apply for joint operations are:

- The Commander in Chief of the Police, Commander in Chief of the Border Guard, or Commander in Chief of the State Fire Service – with the prior consent of the Minister of Internal Affairs;
- The Minister of Internal Affairs – *ex officio* or at the request of the Commander in Chief of the Police, Commander in Chief of the Border Guard, Commander in Chief of the State Fire Service or the Head of the Government Protection Bureau;
- The Prime Minister, at the request of the Minister of Internal Affairs.

Applications should include:

- The purpose and type of joint operation or joint rescue operation;
- The type of assistance that the 'sending' State is to provide to the Republic of Poland;
- The area in which the joint operation or joint rescue operation is to be conducted;
- The anticipated duration of the stay of foreign officers or employees on the territory of the Republic of Poland;
- The type of military or emergency service requested to participate in the joint operation or joint rescue operation;
- The anticipated costs of the joint operation or joint rescue operation and the means of its financing.

Upon acceptance, a detailed list shall be drawn up specifying numerous details, including:

- The purpose and type of activities;
- The nature of the 'sending' state's role;
- A list of foreign officers to be involved;
- The duration of the operation;
- The date the 'sending' state's personnel would cross the border;
- The data of the 'sending' state's participating commanding commanders;
- The number and types of firearms and other necessary equipment to be used;

- The language to be used;
- The costs of the joint operation or joint rescue operation.

In Poland, joint operations can be coordinated by: a regional police chief; a commander of a Border Guard unit; a person designated by the Head of the Government Protection Bureau, or a person designated by the Commander in Chief of the Police, Border Guard or State Fire Service. The choice largely depends on the main force that the officers and employees participating in the operation originate from. If more than one is involved in the operation, it is supervised by the appropriate Commanders in Chief, or by the Minister of Internal Affairs.

Importantly, officers and foreign employees taking part in a joint operation on Polish soil benefit from the same legal protection as Polish officers. They have the right, amongst other things, to:

- Wear a uniform;
- Carry firearms, ammunition and means of direct coercion;
- Use firearms specified in the Anti-Terrorism Act;
- Use the same methods of direct coercion prescribed for Polish Police officers;
- Formally identify people;
- Stop people;
- Collect fingerprints;
- Search people and rooms;
- Perform body searches and searches of luggage and bags;
- Observe and record public events using technical means;
- Request assistance;
- Drive their vehicles as privileged vehicles;
- Use free medical care.

Foreign officers can also use firearms:

- To repel a direct and unlawful attack on the life, health or freedom of foreign officers or employees or other persons;
- In other situations, at the discretion of the commanding officer.

Foreign officers participating in a joint operation enjoy the privileges conferred by Polish law, under the command of, and in the presence of, a Polish officer.

Prior to the commencement of the joint operation, training for foreign officials on the rules of participation in the joint operation must be given, in particular the rules and conditions for the use of firearms and direct coercion.

## **1.8. Organization of activities at the scene of a terrorist incident**

Part 4 of the Anti-Terrorism Act regulates the organisation of anti-terrorist activities at the scene of terrorist incidents. The definition of a terrorist incident scene covers two areas:

- Open or closed spaces in which a terrorist event has occurred or is expected to occur;

- Any space in which a terrorist threat is occurring.

It further defines a ‘terrorist incident’ as a situation in which there is a suspicion of terrorist activity arising from previous terrorist offenses, or a threat to commit such an offense.

Various activities are conducted at the scene of a terrorist incident, and counter-terrorist activities constitute one element of these. Counter-terrorist activities are actions taken against perpetrators or persons preparing or assisting in a terrorist offense, to eliminate the immediate threat to the life, health or freedom of persons or property using specialized forces, tactics and resources.

Counter-terrorist actions have several elements:

- Operational situation – an immediate threat to the life, health or freedom of persons or property by terrorists;

- Target entities – perpetrators, persons preparing or assisting in a terrorist threat or incident;

- Expected result – elimination of the threat to the life, health or freedom of persons or property by terrorists;

- Execution – intervention using specialized forces, tactics and resources.

Polish anti-terrorism law specifies the persons responsible for managing anti-terrorist activities at the site of a terrorist incident in Poland, in order to unambiguously define the responsibilities of all entities involved, not just individual units. For the purposes of these definitions, anti-terrorist actions are defined as one of two kinds:

- Those conducted in and around civilian areas (buildings, streets etc.);

- Those conducted in and around military areas or areas belonging to entities supervised by the Ministry of Defence.

In civilian areas, the responsibilities of responding units are assigned by the Commander in Chief of the Police, or the relevant officer at the local Police Headquarters. In military areas, they are assigned by the Minister of Defence, by the Commander in Chief of the Military Police, or by a Military Police officer.

Commanding officers at terrorist incident scenes have the right to:

- Order the evacuation of persons or property from the area of a terrorist incident to a designated place, building or area;

- Stop or restrict pedestrian traffic and prohibit unauthorized persons from staying at or near a terrorist incident scene;

- Stop or restrict the movement of vehicles at the scene of a terrorist incident or its surroundings, as well as to re-route public transportation vehicles in consultation with the authorities, or re-direct them to a designated location;

- Request the railway authorities to suspend or limit rail traffic at or near a terrorist incident scene, or stop a railway vehicle or re-route it to a designated location;

- Request the port authorities to suspend or limit the water traffic at or near a terrorist incident scene, or to detain a vessel or re-route it to a designated location;
- Request the air traffic authorities to suspend or limit air traffic at airports being the scene of a terrorist incident;
- Demand cost-free use of property or movable property, including means of transport, as well as objects and equipment necessary for carrying out anti-terrorist activities;
- Request assistance from an institution, organization, entrepreneur or natural person, or advise others on how to help minimise or eliminate the effects of a terrorist incident, prevent further terrorist incidents, or detect and identify those responsible for the terrorist incidents.

All persons and entities to whom these orders and demands are directed are legally obliged to comply with them. In the process, the State Treasury bears civil (financial) liability for any damage caused by the anti-terrorist authorities.

### **1.9. Rules of engagement in anti-terrorist operations**

One very important power of the executive is the power to authorise the use of firearms in counter-terrorist activities. In Poland there are two legal acts underlying the use of force by authorized entities:

- Journal of Laws of 2013, item 628 – a general act;
- Journal of Laws of 2016, item 904 – the specific legislation regulating the use of firearms.

The general principle that firearms officers must at all times follow is that of minimising injury, i.e. that weapons should be used in the least detrimental way. Officers must take the necessary precautions, while taking into account the threat to the life and health of their colleagues. Generally speaking, officers cannot be ordered to fire their weapons. Each officer must decide for themselves to fire their weapon and assumes full responsibility for doing so. There are, however, prerequisite conditions for discharging a firearm (including a clear call for cessation of illegal activities, a clear warning that the officer is armed, warning shots etc.). These can be waived only in exceptional cases. After discharging their firearm, the officer must prepare a detailed written report about their use of the firearm during the incident.

Although the two legal acts cited above do not clearly define the situations in which a life can be specifically taken by a firearms officer, the Anti-Terrorism Act does contain a special ‘use of weapons’ formula, according to which officers may legally shoot to kill. This is still an exceptional solution and is, as mentioned in the previous paragraph, constrained by precisely defined restrictions, including:

- Counter-terrorism activities must be conducted in accordance with Anti-Terrorism law;

- Special use of arms should be given to prevent the direct, unlawful, violent assassination of a person's life or health, or to release a hostage;
- The use of weapons on general principles, even in the least detrimental way, is insufficient reasoning to take a kill shot;
- Use of firearms is permitted when counteracting an attack or releasing a hostage in any other way is impossible;
- All of the circumstances of the terrorist incident and the options for countering it must be taken into account;
- Use of firearms is permitted only against persons carrying out an attack or taking or holding hostages.

'Special use' of firearms is carried out under order, after a formal procedure, and only in the context of counter-terrorism. In these situations, there is no obligation to warn about the use of firearms, to give warning shots or to request compliance.

The procedure for allowing special weapons use is:

- Decision to classify the situation as a terrorist event and designate a counter-terrorist authority to take action, made by the competent services or entities as part of their statutory tasks at the scene of a terrorist incident;
- Decision on the admissibility of special use of weapons by the commanding officer at the scene, based on an analysis of the operational situation;
- Decision by the commander of the responding counter-terrorist unit;
- Notification of the decision on the admissibility of the special use of weapons by the relevant authority;
- Issuing of the order by the CT group commander to the officers, on the special use of weapons. The procedure for and purpose of the special use of weapons must be specified in the order.

After the operation, a detailed report on the special use of weapons is made by the commander of the CT forces. The special use of weapons is authorized in the context of counter-terrorist activities only for:

- Police officers;
- Border Guard officers;
- officers of the Internal Security Agency;
- soldiers of the Armed Forces of the Republic of Poland;
- Military Police.

## Rferences

Chomentowski P., *Polski system antyterrorystyczny, prawno-organizacyjne kierunki ewolucji*, Difin, Warszawa 2014.

Council Decision 2008/615 / JHA of 23 June 2008 on stepping up cross-border cooperation, particularly in the fight against terrorism and cross-border crime (Official Journal of the European Union 210 of 6 August 2008).

Council Decision 2008/617 / JHA of 23 June 2008 on improving cooperation between the special intervention units of the Member States of the European Union in crisis situations (EU L 210, item 73).

Jałoszyński K., *Biuro Operacji Antyterrorystycznych Komendy Głównej Policji 1976–2014*, WSPol Szczytno 2014.

Jałoszyński K., *Podsystem kontrterrorystyczny systemu antyterrorystycznego Rzeczypospolitej Polskiej*, [in:] Bogdalski P., Nowakowski Z., Rajchel K., (eds.), *Ocena poziomu zagrożenia terroryzmem i organizacji systemu antyterrorystycznego w Polsce*, WSPol Szczytno, Warszawa 2012.

Jałoszyński K., *Współczesny wymiar antyterroryzmu*, TRIO, Warszawa 2008.

Karwel J., *USA Patriot Act jako przykład ustawodawstwa antyterrorystycznego – analiza i próba ewaluacji. Wnioski dla polskiego systemu antyterrorystycznego*, [in:] Zubrzycki W., Jałoszyński K., Babiński A., (eds.), *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, WSPol Szczytno 2016.

Stępiński M., *Formalno-organizacyjne uwarunkowania dowodzenia działaniami kontrterrorystycznymi realizowanymi przez wyspecjalizowane siły Policji w świetle przepisów ustawy o działaniach antyterrorystycznych*, [in:] Zubrzycki W., Jałoszyński K., Babiński A., (eds.), *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, WSPol Szczytno 2016.

Wojciechowski S., *Terroryzm na początku XXI wieku. Pojęcie, Przejawy, Przyczyny*, Contact, Poznań 2013.

<http://rcb.gov.pl/o-rcb/>

<http://www.antyterroryzm.gov.pl/CAT/antyterroryzm/wspolpraca-zagraniczna/platforma-atlas/579,Platforma-ATLAS.html>

[http://www.coe.int/t/dghl/monitoring/moneyval/About/About\\_MONEYVAL\\_en.asp](http://www.coe.int/t/dghl/monitoring/moneyval/About/About_MONEYVAL_en.asp)

<http://www.consilium.europa.eu/pl/policies/fight-against-terrorism/counter-terrorism-coordinator/>

[http://www.msz.gov.pl/pl/polityka\\_zagraniczna/priorytety\\_polityki\\_zagr\\_2012\\_2016/expose2/expose2017/](http://www.msz.gov.pl/pl/polityka_zagraniczna/priorytety_polityki_zagr_2012_2016/expose2/expose2017/)

[http://www.nato.int/cps/en/natohq/topics\\_77646.htm](http://www.nato.int/cps/en/natohq/topics_77646.htm)

[http://www.nato.int/cps/en/natohq/topics\\_77646.htm](http://www.nato.int/cps/en/natohq/topics_77646.htm)

<http://www.policja.pl/pol/aktualnosci/94461,Porozumienie-w-sprawie-koordynacji-dzialan-na-miejscu-zdarzenia-o-charakterze-te.html>

[http://www.sgdsn.gouv.fr/site\\_rubrique98.html](http://www.sgdsn.gouv.fr/site_rubrique98.html)

<https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/organy-pomocnicze/organy-pomocnicze-rady/128,Miedzyresortowy-Zespol-do-Spraw-Zagrozen-Terrorystycznych.html>

<https://www.abw.gov.pl/pl/zadania/zwalczanie-terroryzmu/centrum-antyterrorysty/62,Centrum-Antyterrorystyczne-CAT.html>