

Threat Assessment of Potential Terrorist Attacks to the Transport Infrastructure

G. Nowacki

Military University of Technology, Warsaw, Poland

ABSTRACT: The paper presents threat assessment of potential terrorist attacks to the transport infrastructure. The range of transportation infrastructure has spread and includes railway, inland waterways, road, maritime, air, intermodal transport infrastructure and intelligent transport systems (ITS). ITS service is the provision of an ITS application through a well-defined organisational and operational framework with the aim of contributing to the user safety, efficiency, comfort and/or to facilitate or support transport and travel operations. Terrorism means acts of violence committed by groups that view themselves as victimized by some notable historical wrong. Although these groups have no formal connection with governments, they usually have the financial and moral backing of sympathetic governments. Typically, they stage unexpected attacks on civilian targets, including transport infrastructure, with the aim of sowing fear and confusion. Based on the analyses, transportation infrastructure is potentially threatened with terrorism attacks, especially road and rail infrastructure (about 23 %), and to a smaller degree the maritime and air transport infrastructure (about 2 %). There were **90,3% of incidents involve land transport (74,5% – vehicles, 9,5% – buses, 6,3% – rail)** covered the 41-year period 1967-2007 in the USA. Legal steps to fight terrorism have been taken on the international level, furthermore, some institutions have been established for this purpose.

1 INTRODUCTION

The development of civilisation, scientific and technical progress and new geopolitical situation in the world, cause the forms and means of threat to change.

The most serious danger among new threats to the international system and safety of individual countries, including Poland, creates international organised terrorism and organised crime, although the degree of danger to the individual countries is different. Terrorist attacks are directed at important persons, institutions and countries to cause destruction or panic. Unidentified explosive charges

are used for that purpose, are simple home-made or remotely controlled.

Transport infrastructure is becoming real threat of terrorists attacks, especially land transport including subways, railroad trains, busses and bridges.

Unlike airlines, where security checkpoints screen passengers and luggage, mass transit options like passenger trains, subways and buses, are designed to be easily accessible and are therefore harder to protect. The most likely kind of attack on subways or buses would involve setting off conventional bombs, the materials and know-how are readily available (Targets for Terrorsim, 2006). Less likely but far more devastating scenarios involve the release of a chemical agent such as sarin gas or a biological

agent such as anthrax or smallpox into a subway system. Terrorists could also derail a passenger train or blow up a bridge or tunnel, killing many people and crippling a city's infrastructure for months or even years (Targets for Terrorism, 2006).

Modern transport system must therefore be least susceptible to dangers and durable from the economic, social and environmental protection point of view.

Building future plans of the transport sector development, it is necessary to be aware of its economic significance. Total expenditure for this sector, about 1 000 billion EURO, represents over 10% EU gross product. It determines development of infrastructure and technology, whose cost to the society is not a subject of questioning. Due to the significance of the expenditures in transport and their particular role in the economic growth, the authors of the Rome Treaty have foreseen creating joint policy, subject to specific regulations.

Transport infrastructure represents a basis for functioning of the economy and its development should be shaped with a care to the modernity and effectiveness, especially taking into account considerable costs of this development. The important reason is ensuring functional and developmental coherence on the mainly European scale.

The transport networks, thanks to the fact that they facilitate the flow of people, freight, increase the possibilities of the trade exchange, affect integration of the domestic markets – make it possible for individual regions to develop.

The European program of activities for the road traffic safety defines main areas of actions, and among them better protection of cars by introducing new technical solutions and improving road infrastructure thanks to the application of the intelligent transport systems.

2 THE TRANSPORT INFRASTRUCTURE

2.1 *The terminology of the transport infrastructure*

The infrastructure is a group of the essential equipment and institutions, necessary for a correct functioning of the economy and society (Schmid & Jongman 1988, Encyclopaedia 1982).

In view of W. Mirowski, the infrastructure is an international term, meaning a group of essential objects, equipment and institutions of a service character necessary for the correct functioning of the society and production branches of economy (Mirowski 1996).

Transport is a transfer of people, freight in space using appropriate means (Rydzkowski & Wojewódzka-Król 2008). Transport is closely linked with the remaining branches of economy. Its development is a condition for their development and vice versa – the worsening of economical or transport development is associated with worsening of the situation in respectively transport and economy.

The transport infrastructure is mainly created by the three essential groups:

- routes of all types of transport (road, railways, inland waterways, maritime and air),
- transport junctions (intersections, airports, ports, rail stations, intermodal terminals, logistics centres, etc.),
- auxiliary equipment for the direct servicing of routes and transport junctions.

The term „transport infrastructure“ and its scope have been defined in the Union legislation and have not changed for a long time, practically since 1970 till 2011. According to the Regulation (EEC) No 1108/70 of the Council of 4 June 1970 and Regulation (EEC) No 2598/70 of the Commission of 18 December 1970 and Commission Regulation (EC) No 851/2006 of 9 June 2006, the transport infrastructure means all roads and permanent equipment for the three types of transport, which are necessary for ensuring flow and safety of traffic.

The definition and scope of the transport infrastructure will be changed this year, based on the final proposal for a Regulation of the European Parliament and of the Council on Union guidelines (COM 650 final 2011/0294) for the development of the Trans-European Transport Network concerning union guidelines for the development of the trans-European transport network (planned date of acceptance - March 2012).

2.2 *The types of the transport infrastructure*

According to a new decree, the transport infrastructure, including that of trans-European transport network, consists of:

- Railway transport infrastructure,
- Inland waterways infrastructure,
- Road transport infrastructure,
- Maritime transport infrastructure,
- Air transport infrastructure,
- Multimodal transport infrastructure,
- Equipment and intelligent transport systems associated with the transport infrastructure.

ITS means systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport (Directive 2010/40/EU; Nowacki 2012).

On the 16 of December 2008 the European Commission published Announcement - Plan of the introduction of the intelligent transport systems in Europe, COM (2008)886, which found its reflection in the Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010, M/453 mandate of 6 October 2009 and Commission Implementing Decision 2011/453/EU of 13 July 2011 executive decision.

From the presented analysis of the subject literature it transpires that the scope of the transport infrastructure will widen, and additionally, in each of the infrastructure category the intelligent transport systems have been highlighted.

Transport infrastructure as a potential target of terrorist attack should be a critical input into risk management policy regarding risk allocation decisions. Terrorism attack on transport infrastructure can cause collateral damage to neighbouring environment, including massive economic and social consequences that rely upon that infrastructure.

Transport infrastructure protection might include major highways, bridges, railways, and it also typically addresses air transportation, including air traffic control operations and airport security as well as waterways.

3 CHARACTERIZATION OF TERRORISM

3.1 *The term and essence of terrorism*

Terrorism is not a new phenomenon, but is a variable, multi-level and dynamic one, as among the others, the forms, means and objectives of the terrorist activities, change. The terrorism phenomenon is affected by the civilization development and scientific and technical progress, especially as far as new communication means, mass media and advanced communication technologies are concerned.

The US Defence Department defines the terrorism as unlawful use or the threat of using force or violence against people, property, to pressurize or scare the governments or societies to achieve political, religious or ideological aims (Aleksandrowicz 2008).

The term – terrorism, should be understood solely as the use of violence by the individuals or groups of people, to exert the pressure both on the government and public opinion as well as the groups of people and individual persons (Olechów 2002).

A. Schmidt defined the classic terrorism, as an attack of a subversive forces on the innocent individuals, aimed at causing fear, kill or injure people, and thus force the political concessions from a person or organisation not actually being a direct victim of an assault, and to which the attacked individuals do not belong. (Schmidt 1988). This criterion was used in 1988 by Alex Schmid and Albert Jongman. They made a statistical analysis of 109 terrorism definitions and concluded that the most frequently occurring elements of terrorism are (Schmidt & Jongman 1988) – Fig. 1:

- violence/force – 83,5%,
- political aspect of the phenomenon – 65%,
- fear – 51%,
- threats – 47%,
- psychological effect – 41,5%,
- existing discrepancies between the target and victim – 7,5%,
- planned, purposeful, systematic and organised actions – 32%,
- fighting, strategic and tactical methods – 30, 5%.

According to the UN, the terrorism (Latin) are various ideologically motivated, planned and organised actions of individual people or groups resulting in violating the existing legal order, undertaken for the purpose of forcing the state authorities and society into certain behaviours and benefiting actions, often violating the welfare of the

outsiders. These actions are performed with an utmost ruthlessness, by various means (physical violence, use of weapons and explosions), in order to give them maximum publicity and intentionally causing fear in the society (The report of UNIC 2012).

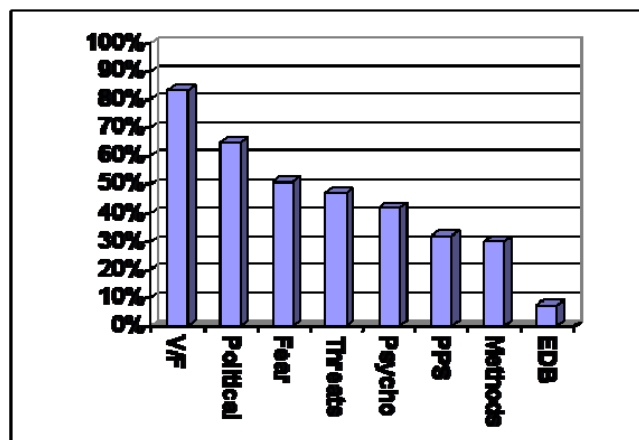


Figure 1. The most frequently occurring elements of terrorism (Schmid, A. P. and Jongman, A. 1988)

According to the Criminal Code (The act from 16 April 2004) the crime of a terrorist character is a forbidden act punishable by an imprisonment, whose limit is at least 5 years, and which is committed in order to:

- seriously frighten many people,
- force the public authorities of the Republic of Poland, other countries or the international organisation authorities, to undertake or abandon certain activities,
- cause serious disturbances in the political system or the economy of the Republic of Poland, other countries or the international organisation – as well as the threat of committing such an act.

The main forms of the terrorist attacks are (Pawłowski 1994):

- assault against life – is directed most often against important persons, political party leaders,
- bomber attack – exerts specific psychological pressure on the society,
- hijacking vehicle or plane,
- taking hostages, kidnapping – serves the purpose of using them as a trade over element in meeting the demands.

It needs to be noted also that 95 % terrorist attacks in the world were conducted using explosives.

According to RMS' historical catalogue of macro terrorism attacks (defined as attacks with the minimum severity of a car bomb), the terrorist violence has increased substantially since 2001 (Coburn & Paul & Vyas & Woo & Yeo 2012). More than 2 400 macro attacks have occurred worldwide since 2001, killing over 37 000 people and injuring nearly 70 000.

The Institute for Economics and Peace (IEP) has indicated in its inaugural global terrorism index of 158 countries, that only 31 have had no attacks in the ten years from 2002 to 2011 (Institute for Economics & Peace 2012). Yet although the attacks are distributed widely around the world, the majority are concentrated in just a handful of countries. Iraq ranks

first weighted average of the number of incidents, deaths, injuries and estimated property damage. Other terrorist hotspots include Pakistan, Afghanistan, India and Yemen (Tab. 1).

Table 1. Global terrorism index from 2002 to 2011 (Institute for Economics & Peace. Dec 4th 2012)

Rank	Country	Score
1	Iraq	9.56
2	Pakistan	9.05
3	Afghanistan	8.67
4	India	8.15
5	Yemen	7.31
6	Somalia	7.24
7	Nigeria	7.24
8	Thailand	7.09
9	Russia	7.07
10	Philippines	6.80

The total number of terrorist attacks and terrorism-related arrests in the EU continued to decrease in 2011. The main figures for 2011 are:

- 174 terrorist attacks in EU Member States,
- Lone actors were responsible for the killing of 2 persons in Germany, and 77 persons in the non-EU country Norway.

The total number of terrorist attacks in the EU has decreased to 219, but 17 people were killed.

3.2 Terrorist attacks conducted on the transport infrastructure objects

Facilities accessible to large numbers of people, such as transport infrastructure facilities and vehicles are vulnerable to attack by vandals, extremists, terrorists, and other criminals. For example, the March 11, 2004 Madrid commuter train bombings by terrorists inspired by Al-Qaeda killed nearly 200 people and wounded 1 800. And, on the morning of July 7, 2005, four suicide bombers successfully detonated bombs on the London Underground, killing 52 people and injuring over 700 (Coburn & Paul & Vyas & Woo & Yeo 2012).

In view of the Aon Global Risk Consulting experts, the most often targeted trade by the terrorists was retail trade - 24, 18% (The report of Aon 2008) - Tab. 2.

Affected were not only the shopping centres or supermarkets, but also small gastronomy outlets, restaurants, clubs and bars. It is possible to indicate three main reasons for the terrorist attacks in the retail sector. First of all, vast part of them is directed at the shops owned by non-Islamic people.

Secondly, the terrorists often chose renowned makes as the target of their attacks, which are a symbol of the western world and capitalism. And thirdly, the retail trade is an attractive target for the attacks of the terrorist groups due to the possibility of causing significant human losses, serious difficulties in the everyday life and an effective scaring of the civilian population.

Table 2. Terrorism attacks on various trade

Various trade	%
Retail trade, gastronomy	24,18%
Land transport (road, railways)	23,36%
Mining industry	14,55%
Infrastructure (objects of the state authorities, local governments, public, religious cult)	8,2%
Construction	5,74%
Tourism	6,56%
Finances	2,05%,
Air transport	2,46%
Maritime transport	2,25%
Public utility enterprises	2,25%
Other	8,4%

The second place on the list of the terrorist attacks takes road and railways transport infrastructure (23, 36%).

The selected terrorist attacks conducted in 1970-2011, are presented in the table 3.

Table 3. Selected terrorist attacks carried out on the transport infrastructure objects

Place, date	Type of attack	Victims
Israel, 8 May 1970.	PLO attack on the school bus.	9 children and 3 adults died and 19 were injured.
Switzerland – Israel, 21 February 1970	Bomb explosion in on board of the Swissair 330 airliner.	47 people died.
Yugoslavia 26 January 1972.	Attack on the DC-9 aircraft of the Yugoslav airline.	27 people died (23 passengers and 4 crew members).
Israel 30 May 1972	Bomb attack at the Lod airport in Israel	26 people died, 78 were injured.
India, 23 June 1985	Bomb attack on board of the Boeing 747	329 people died.
Japan, 20 March 1995.	Attack on Tokyo underground, using sarin gas.	13 people died, 5 thousand were seriously intoxicated
USA, 11 September 2001.	Attack on WTC and Pentagon.	2973 people died, 19 hijackers and 26 people were missing
Spain, 11 March 2004.	Bomb attack in Madrid underground.	191 people died, 1900 were injured.
Russia, 6 February 2004.	Bomb attack in Moscow underground.	41 people died, and over 100 were injured.
G. Britain, 7 July 2005.	Bomb attack in London underground.	52 people died, and at least 700 were injured.
India, 19 February 2007	Bomb attack express train.	68 people died, many were injured.
Africa, 8 January 2010.	Coach carrying Togo soccer players to an African nations Cup machine gunned.	At least 195 people died, about 300 were injured.
Russia, 29 March 2010.	Bomb attack on underground in the centre of Moscow, carried out by two suicide women.	At least 39 people died, and 102 were injured
Russia, 24 January 2011	Bomb attack at the Domodiedowo airport.	36 people died, and at least 180 were injured
Belarus, 11 April 2011.	Bomb attack in Minsk underground.	15 people died, and 204 were injured

Transport infrastructure is a frequent target of terrorist attacks because of its significance in several dimensions (Zeng & Chawathe & Wang 2007). Because physical transportation networks attract large numbers of people, they're a high value targets for terrorists intending to inflict heavy casualties. Transport infrastructure is important to the modern economy, and related damages and destruction can have quick ripple effects. Operationally, transportation systems interact with and provide support for other systems, such as emergency response and public health, in complex ways. Terrorists can perceive an attack on such a link (that is, one that connects many systems) as an efficient means to create confusion, counter the countermeasures, and damage the targeted society as a whole. Furthermore, transport infrastructure can be both the means and the end of an attack, making them a critical part of almost all terrorist attacks in the physical world.

Tab. 4 shows the yearly counts of transportation related terrorist incidents from 1998 to 2004, broken down by transportation mode.

Table 4. Terrorism incidents by transportation mode (Zeng, D., Chawathe, Sudarshan, S., Wang, FeiYue, 2007)

Year	Transportation mode		
	Maritime	Air	Land (road and rail)
1998	1	7	36
1999	2	9	54
2000	2	11	56
2001	2	12	28
2002	0	10	41
2003	1	5	41
2004	2	5	25

Susan Pantell has presented terrorist attacks involving transport infrastructure, especially vehicles and facilities being tallied and covered the 41-year period 1967-2007 in the USA (Fig. 2).

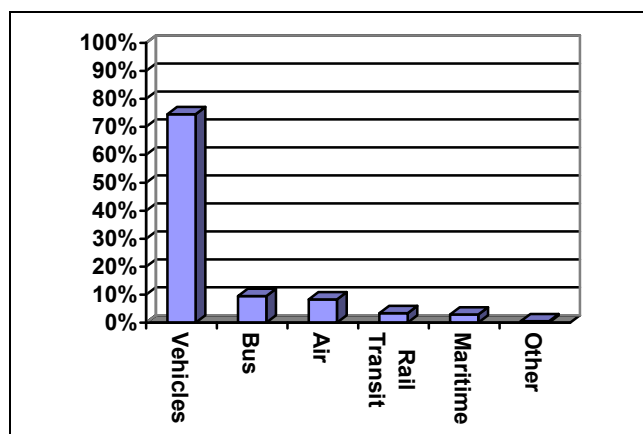


Figure 2. Terrorist incidents involving transport infrastructure in USA (Light Rail Now Project, 2008)

According to presented data, 90,3% of incidents involve land transport (74,5% – vehicles, 9,5% – buses, 6,3% - rail), 8,3% - air transport, only 0,9% maritime transport and 0,5% other.

Air transport (8,3 %, which clearly has been shown to be quite vulnerable, and, along with motor vehicles, a favoured target – and instrument – of

terrorists) has been subjected to a comparatively rigorous security crackdown; on the other hand, private motor vehicles movement has been subjected to basically nothing in terms of comparable ongoing security measures.

Recent terrorist attacks on transport infrastructure have highlighted the vulnerability of road and rail networks, reinforcing the importance of good risk assessments to protect some of our biggest assets.

Throughout the European Union there are five million kilometres of road, and among them:

- 65 000 km of these being motorways,
- 212 000 km rail lines,
- as well as 42 000 km of navigable inland waterways.

According to Brian D. Taylor, director of the Institute of Transportation Studies at the University of California (UCTC 2010), acts of terrorism intersect with transport infrastructure in three ways:

- When transportation is the means by which a terrorist attack is executed,
- When transportation is the end, or target, of a terrorist attack,
- When the crowds that many transportation modes generate are the focus of a terrorist attack.

4 COMBATING TERRORISM

4.1 Tasks to combat terrorism

Transport infrastructure is inherently vulnerable to terrorist attacks, as it is an open area that gathers large numbers of people at predictable times in predictable places.

As defined earlier, transport infrastructure includes physical facilities, equipment, assets, service networks, and communication and computing hardware and software that enables information access and transactions (Zeng & Chawathe & Wang 2007).

Transport security encompasses mass passenger transport systems such as roads, bridges and tunnels, bus terminals and rail stations, trams, and air cargo supply chains and maritime ports. From the mentioned aspects, transport infrastructure security tasks should include relevant application context as follows:

- physical access management and control of employees and passengers,
- perimeter intrusion detection,
- vulnerability assessment,
- intrusion detection and access control in the cyberspace in which pertinent information systems operate and exchange data,
- related simulation and decision support tools.

Transport plays an important role in the economic growth and globalization because of connecting to other economy sectors.

Transport infrastructure security is the complex of roles, responsibilities and relationships in the different sectors (Roads, Railways, Inland waterways, Air and Maritime, Multimodal) and refers to other economy sectors. Thus transport infrastructure

security management against terrorist attacks, needs multi agency and multi jurisdictional domain, regulatory, law enforcement and intelligence agencies on international and national levels.

4.2 *International institutions to fight terrorism*

UN has taken many efforts to fight terrorism since 1963 and accepted many conventions. Security Council created Counter-Terrorism Committee Executive Directorate (CTED) based on resolution 1535 from 2004. General Secretary appointed UN Counter-Terrorism Implementation Task Force - CTITF in 2005.

On 8 September 2006 all UN member states accepted Global Strategy of Combating Terrorism. For the first time in history a joint stand has been agreed on combating terrorism. Accepting Global Strategy of Combating Terrorism crowns years of efforts and at the same time fulfils the obligation made by the world leaders at the World Summit in September 2005. While developing strategy, many proposals and recommendations presented by a former Secretary General Kofi Annan were taken into account.

The basis for the strategy is unequivocal, unconditional and firm condemnation of terrorism in all its forms – used by anybody, anywhere and for whatever reasons. The strategy establishes concrete measures, that are to be taken in order to eliminate causes for spreading terrorism and to strengthen individual and joint capability of nations and United Nations in preventing and combating terrorism, protecting simultaneously human rights and legal rules.

The strategy combines many new proposals and strengthenings of the current actions taken by the member states, UN system and other international and regional institutions into a common platform of strategic co-operation.

The General Assembly reviewed the implementation of the United Nations Global Counter-Terrorism Strategy on 28-29 June 2012 at the UN headquarters in New York. The Strategy refers to activities of four pillars, which are:

- 1 Addressing conditions conducive to the spread of terrorism,
- 2 Preventing and combating terrorism,
- 3 Capacity-building to prevent and combat terrorism,
- 4 Respect for human rights and the rule of law.

The terrorism creates direct danger to the safety of the NATO states and for the international stability and welfare. The terrorist groups infiltrate and propagate in the areas of a strategic significance to the Alliance, modern technology causes increase of the danger and potential threat of the terrorist attacks, especially if the terrorists were to come into possession of the nuclear, chemical, biological or radiological capabilities.

At the NATO level operates EADRCC (Euro-Atlantic Disaster Response Coordination Centre), created in June 1998, at the NATO Head Quarters, based on the motion put forward by the Russian Federation. Created, as part of the Partnership for

Peace program, Centre co-ordinates NATO the partner states' actions in the area of the Euro-Atlantic in a reaction to natural disasters and those caused by a man. All those tasks are conducted in a close co-operation with the UN Office for the Co-ordination of Humanitarian Aid (UN OCHA), which has been entrusted with a superior role in co-ordinating international actions during disasters. Since 2001 EADRCC has played a role in co-ordinating the reaction of the countries to a terrorist attacks with the use of chemical, biological or radiological weapons, as well as the activities managing the consequences of those events.

The Military Concept for Defence against Terrorism and the Partnership Action Plan Against Terrorism were taken in Prague Summit in 2002. The Terrorist Threat Intelligence Unit – (TTIU) was created in Istanbul Summit in 2004.

The Euro-Atlantic Partnership Council's Partnership Action Plan against Terrorism, launched at Prague, is updated annually. The Alliance set another important milestone at the November 2006 Riga Summit by endorsing a Comprehensive Political Guidance that highlights the threats posed by terrorism and the spread of weapons of mass destruction, among others (Steinhäusler, F., Edwards F. 2005).

A fully operational NATO Response Force (NRF) can be used to fight against terrorism. The NRF will serve as a catalyst for transformation and interoperability, and by doing so will enhance the quality of Allied armed forces whether they be used for NATO, EU, UN or national operations. At Riga, member countries expressed their support for mechanisms to ensure long-term force generation and to allow for a more sustainable and transparent approach to maintain the Force's future capabilities. While neither the NRF nor the recently-approved Special Operations Forces Transformation Initiative are intended to be used exclusively for counter-terrorism purposes, they enhance the Alliance's ability to mount expeditionary operations. This capability, in turn, will invariably prove useful in confronting threats that originate within failed states (Steinhäusler, F., Edwards F. 2005).

The 2010 Strategic Concept threats include the proliferation of nuclear weapons, terrorism, cyber attacks and key environmental and resource constraints. NATO has adopted a holistic approach to crisis management, envisaging NATO involvement at all stages of a crisis. NATO will therefore engage, where possible and when necessary, to prevent crises, manage crises, stabilize post-conflict situations and support reconstruction.

In accordance with a strategic concept of defence and safety of the members of the NATO treaty, the Alliance takes on itself obligation to prevent crises, terrorist threats, managing conflicts and stabilising post-conflict situations, including closer co-operation with international partners, especially United Nations Organisation and European Union.

The European Council on the 25 March 2004 accepted the Declaration and a Plan, being an annex to the Declaration, on combating terrorism. One of the most important provisions is an acceptance of, so

called, solidarity cause. It envisages, that in case of the terrorist attack on any EU member state, all remaining members will mobilise every available means, they regard as appropriate (including military ones), to help the state in trouble. In the declaration, there is a reference also to the European Security Strategy of December 2003, in which the terrorism was regarded as one of the most serious dangers to the international security.

The 2010 Strategic Concept threats include the proliferation of nuclear weapons, terrorism, cyber attacks and key environmental and resource constraints. NATO has adopted a holistic approach to crisis management, envisaging NATO involvement at all stages of a crisis. NATO will therefore engage, where possible and when necessary, to prevent crises, manage crises, stabilize post-conflict situations and support reconstruction.

The European Council on the 25 March 2004 accepted the Declaration and a Plan, being an annex to the Declaration, on combating terrorism. One of the most important provisions is an acceptance of, so called, solidarity cause. It envisages, that in case of the terrorist attack on any EU member state, all remaining members will mobilise every available means, they regard as appropriate (including military ones), to help the state in trouble. In the declaration, there is a reference also to the European Security Strategy of December 2003, in which the terrorism was regarded as one of the most serious dangers to the international security.

At the EU level there has been Monitoring and Information Centre (MIC) established, which is available and capable of an immediate reaction, 24 hours a day, and also serving the member states and the European Commission to react to dangers. The Centre serves 31 states (28 EU states and Lichtenstein, Iceland and Norway).

More over, the Common Emergency Communication and Information System (CECIS) is used in the Crises Situations in order to enable the communication between MIC and the contact points in the member states as well as sharing by them the information and managing them.

The Schengen zone countries use Schengen Information System – SIS, and the access to the system is in the possession of the police, consular offices and Border Guard together with Customs Offices and it enables the verification of people during the border control as well as during the control within the country.

The Counter-Terrorism Coordinator (CTC), the Counter Terrorism Group (CTG) and the Joint Situation Centre (SITCEN) were appointed to fight terrorism in the European Union.

At the EU level there have been independent institutions: Europol, Eurojust and Frontex.

Europol (European Police Office) is the European Union law enforcement agency that handles the exchange and analysis of criminal intelligence in preventing terrorism and serious international crime in order to raise the safety within the entire Europe. Europol commenced its full activities on 1 July 1999.

Eurojust (The European Union's Judicial Cooperation Unit) is a body established in 2002 to stimulate and improve the co-ordination of investigations and prosecutions among the competent judicial authorities of the European Union Member States when they deal with serious cross-border and organized crime.

Frontex (Franch: *Frontières extérieures*) is a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. Frontex started to be operational on October 3, 2005 and is headquartered in Warsaw.

On the wide international forum, INTERPOL has been used (190 countries) – the police organisation of the EU countries and those from outside the Union, e.g. Belarus, Russia, Ukraine. The co-operation takes place as part of the liaison officers network of the Polish Police operating in such EU countries as France, Holland, Germany, Great Britain, and countries outside the Union, i.e. Belarus, Russia, Ukraine. They have a direct access to the police data bases (lost and wanted persons, dactyloscopic cards, DNA profiles, stolen vehicles and documents, etc.).

4.3 National institutions

In Poland combating terrorism is dealt with by the following institutions (Strategy of National Security for the Republic of Poland 2007):

- at the strategic level: Government Centre for Security (GCS), National Crisis Management Team (NCMT), Interdepartmental Team for the Terrorist Threat (ITTT), Internal Security Agency (ISA), Intelligence Agency (IA), Military Intelligence Service (MIS), Military Counter-Intelligence Service (MCIS), Police Head Quarters (PHQ), Border Guard Head Quarters (BGHQ), Chief Inspector for the Financial Information (CIFI), Customs Service (CS), State Fire Service Head Quarters (SFBHQ), Government Protection Bureau (GPB), Military Police Head Quarters (MPHQ), General Staff of the Polish Armed Forces, National Atomic Energy Agency (NAEA), Civil Aviation Authority (CAA), Polish Air Navigation Services Agency (PANSAs);
- at the operational level: Counter-Terrorist Centre (Makarski 2010, CTC 2012). The CTC operates in a twenty-four-hour system, 7 days a week. It comprises, apart from officers of the Internal Security Agency, seconded officers, soldiers and employees of e.g. the Police, the Border Guard, the Government Protection Bureau, the Foreign Intelligence Agency, the Military Intelligence Service, the Military Counterintelligence Service and the Customs Service. They carry out tasks within competences of the institution which they represent. Furthermore, together with the Counter – Terrorist Centre actively cooperate other bodies which participate in the system of anti-terrorist protection of the Republic of Poland such as: the Government Centre for Security, the Ministry of Foreign Affairs, the State Fire Service, the General Inspector of Financial Information, the General Staff of the Polish Armed Forces, the Polish Military Gendarmerie etc. The essence of the CTC

functioning system is coordination of the information exchange process between the antiterrorist protection system participants, enabling implementation of the common procedures for reacting at the occurrence of one of the four categories of the defined threat:

- terrorist threat occurring outside the Polish borders but affecting the security of the RP and it's citizens,
 - terrorist occurrence taking place on the Polish territory affecting the security of the RP and it's citizens,
 - information obtained about a potential threats that may take place on the Polish territory outside the Polish borders,
 - information obtained concerning laundering money or transferring financial resources that may be a proof of financing the terrorist activities.
- at the tactical level: special units, services and institutions answering to the Internal Affairs Minister (IAM), National Defence Minister (NDM), Financial Minister (FM), Minister of Transport, Construction and Maritime Economy (MTCME), special units.

Intelligence and counter-intelligence tasks of the special services (ISA, IA, MIS, MCIS) concern recognising and counteracting the internal and external occurrences, which threaten the state's interests. The essential role of the special services relies on obtaining, analysing, processing and conveying to the correct authorities, the information, which can be of considerable significance for the state security in every aspect, as well as on the pre-emptive informing about the potential and existing threats to the country. Special attention is given to preventing and counteracting the terrorism, protecting the defence and economic capabilities of the country, being a condition for it's international position. The special services ensure the counterintelligence protection of the country, especially in respect to the functioning of the main elements of the critical infrastructure, including transport networks.

The superior objective of the Police actions is to serve the society by effectively protecting the security of people and property as well as maintain security and public order. The Police prevent crime and criminogenic phenomena, including those of a cross-boarder character, co-operating with other guards, services and state inspections as well as the police of other countries together with the international organisations. The Police are prepared also for providing a wider support to missions conducted by other state and non-governmental entities, as well as the Armed Forces of RP. Preventing and effective response to the cases of organised crime should remain the care of not only the Police, but also other services and departments. Polish police should actively participate and initiate solutions at the international institutions of the police co-operation, such as Interpol or Europol, and develop the network of its liaison officers, actively representing Polish police outside the country.

As the priority actions, should be regarded the co-operation of the Police law enforcement bodies, Internal Security Agency with the Anti-Terrorist

Centre, for the purpose of eliminating the terrorist and criminal events.

The superior objective of the Border Guard is an effective protection of the state borders and controlling the boarder traffic in accordance with the interests of the state security interests. It's special role is to protect one of the longest land sections of the external boarder of, both the European Union and NATO, as well as the responsibilities resulting from signing the Schengen Treaty by Poland.

It is necessary to continue and improve co-operation between the Border Guard, the Police and other services. The monitoring and migration control of the foreigners on the entire territory of the country is an important area requiring the intensification of the co-operation of these services, which should also have a preventive character. Both the Police and the Border Guard, as part of the statutory activities, ought to constantly monitor the threats of a terrorist character, co-operating in that, with other services.

The superior objective of the State Fire Service is recognising threats, preparing and carrying out the rescue actions. The SFS possesses the capability to immediately respond in cases of a threat to life and health, environment and property as well as in the cases of the extraordinary threats, disasters and natural disasters.

5 CONCLUSIONS

The terrorist attacks threats to the transport infrastructure are quite significant world-wide, and so far this trade attracted about 24% of all attacks carried out.

According to intelligence agencies, criminals and terrorists are planning to disrupt transport infrastructure in different countries all over the world because it is the open area that gather large numbers of people at predictable times in predictable places.

The tasks referring to protecting people and transport infrastructure while allowing transport systems to operate efficiently and effectively, should become a national and international priority. The solution requires global initiatives and close co-operations of transport operators, police, security and other international organizations, including the UN, NATO and European Commission.

The state services of the Republic of Poland are well prepared to recognise, prevent and combat terrorist threats. The most important is the co-operation of all services as well as an early recognition of the threat and not allowing the terrorist attack to take place (prevention).

More over, it would be advisable to prepare guide books concerning the behaviour of people in the crises situations, especially about the symptoms of the terrorist attack, being prepared, and the ways the people should behave in such cases.

REFERENCES

- Aleksandrowicz, T. R. 2008. International terrorism, Warsaw.
- Coburn, A. and Paul, M. and Vyas, W. and Woo, G. and Yeo W. 2012, Terrorism Risk in the Post-9/11 Era. A 10-Year Retrospective. Risk Management Solutions, Inc. Newark, USA.
- CTC. Counter Terrorism Centre of the Internal Security Agency in The Republic of Poland. http://www.antyterroryzm.gov.pl/portal/eng/265/621/COUNTER_TERRORIST_CENTRE_CTC.html.
- Commission Implementing Decision 2011/453/EU of 13 July 2011 adopting guidelines for reporting by the Member States under Directive 2010/40/EU of the European Parliament and of the Council (notified under document C2011/4947). OJ of the EU, L 193/48, 49 of 23/7/2011.
- Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. OJ of EU, L 207, 06/08/2010 P. 0001 – 0013.
- Encyclopaedia PWN. 1982. PWN, Warsaw.
- Global terrorism index. Capturing the Impact of Terrorism for the Last Decade. IEP. Dec 4th 2012. <http://www.visionofhumanity.org/wp-content/uploads/2012/12/2012-Global-Terrorism-Index-Report1.pdf>.
- Makarski, A. 2010. Genesis, activities, rules and experiences after one year functioning of Anti-Terrorist Centre. Review of Internal Security, No 2. Anti-Terrorist Centre, Warsaw. http://www.abw.gov.pl/portal/pl/273/642/Przeglad_Bezpieczenstwa_Wewnetrznego_nr_2_2_2010.html.
- Mandate 453 EN (2009). Standardization mandate addressed to CEN, CENELEC and ETSI in the field of information and communication technologies to support the interoperability of co-operative systems for Intelligent Transport in the European Community. Brussels, 6th October 2009. DG ENTR/D4.
- Mirowski, W. 1996. Study on Polish country infrastructure. The equipment areas of social infrastructure. T. III. PAN Instytut Rozwoju Wsi i Rolnictwa, Warszawa.
- NATO 2010. Strategic Concept for the Defense and Security of The Members of the North Atlantic Treaty Organization, Adopted by Heads of State and Government in Lisbon, Nov. 2010. <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>.
- Nowacki G. 2012. Development and Standardization of Intelligent Transport Systems. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. 6, No. 3, pp. 403-411.
- Olechów, B. 2002. Terrorism in after bipolar World. Adam Marszałek, Toruń.
- Pawłowski, A. 1994. Terrorism in Europe of XIX & XX century. Lubuski Komitet Upowszechniania Prasy, Zielona Góra.
- Regulation (EEC) No 1108/70 of the Council of 4 June 1970 introducing an accounting system for expenditure on infrastructure in respect of transport by rail, road and inland waterway. OJ L 130, 15.6.1970, p. 4–14 .
- Regulation (EEC) No 2598/70 of the Commission of 18 December 1970 specifying the items to be included under the various headings in the forms of accounts shown in Annex I to Council Regulation (EEC) No 1108/70 of 4 June 1970. OJ L 278, 23.12.1970, p. 1–5.
- Regulation (EC) No 851/2006 of 9 June 2006 specifying the items to be included under the various headings in the forms of accounts shown in Annex I to Council Regulation (EEC) No 1108/70. OJ L 158, 10.6.2006, p. 3–8.
- Rydzkowski, W. and Wojewódzka-Król, K. (red.). 2008. Transport. PWN, Warszawa.
- Schmid, A. 1988. Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature. New Brunswick, NJ 1988.
- Schmid, A. and Jongman, A. 1988. Political terrorism. SWIDOC, Amsterdam.
- Steinhäusler, F., Edwards F. 2005. NATO and Terrorism: Catastrophic Terrorism and First Responders. Springer, 2005.
- Strategy of National Security for Republic of Poland, Warsaw, 2007.
- Targets for Terrorism: Ground Transportation. July 13, 2006, <http://www.cfr.org/homeland-security/targets-terrorism-ground-transportation/p10198>.
- The act from 16 April 2004 – Penal Code (Kodeks Karny) and others acts. OJ. 2004, No 93, pos. 889.
- The report of Aon Global Risk Consulting, <http://forsal.pl/wiadomosci/polska/341600.html> <http://www.aon.com/poland>, 2008.
- The report of UNIC from 10.02.2012, <http://www.unic.un.org.pl/terroryzm/definicje.php>.
- Terrorist Attacks and Transport Systems. Institute of Transportation Studies at the University of California. 2010. <http://www.uctc.net/access/28/AccessComment/TerroristAttacksandTransportSystems.pdf>.
- Terrorist attacks mapped around the world. 2012. Institute for Economics & Peace, New York. 13 December 2012. <http://www.economist.com/blogs/graphicdetail/2012/12/daily-chart-0>.
- US LRN. 2008. Light Rail Now Project. http://www.lightrailnow.org/features/f_lrt_2008-06a.htm.
- Zeng, D. and Chawathe, S. and Wang, F.Y. 2007. Protecting Transportation Infrastructure. ITS Department. IEEE Intelligent Systems, July/August 2007.