NATIONAL SECURITY

CRITICAL INFRASTRUCTURE SECURITY IN POLAND AND THE SURROUNDING AREA. LEGISLATION ANALYSIS.

Zbigniew GRZYWNA[1], PhD

Abstract

The Critical Management Act creates a legal basis for dealing with critical infrastructure. It contains the following definition: critical infrastructure includes systems and functional objects which are connected with each other, including: buildings, devices, systems, key services for a country and its citizens' security and other systems and objects which deal with ensuring efficient functioning of public administration bodies as well as institutions and enterprises. At national level, the protection of critical infrastructure is coordinated by the Government Centre for Security[2]. In accordance with the critical management act, which is in effect at present, the legislator defines that critical infrastructure is created by systems and consists of functional objects connected with each other: buildings, devices, systems, key services for a country's security and its citizens' security and other objects and services which deal with ensuring efficient functioning of public administration bodies as well as institutions and enterprises The article contains an enumeration of the systems which are included in critical infrastructure.

Key words: Management safety, critical situation, critical infrastructure, public administration

1 Col. PhD. Zbigniew Grzywna is a pro vice-chancellor in Silesian School of Economics and Languages in Katowice, Director of Management Department.

2 http.//Infrastruktura_krytyczna#regionalne_programy_ochrony_infrastruktury_krytycznej.

The influence of threats on the functioning of infrastructure

In order to make an individual analysis it is necessary to assess the work of those responsible for security. Therefore, this article was created on the basis of analyses. The intention of the legislators who are responsible for security was to limit the documentation of critical response procedures to an essential amount of documentation which makes it possible to manage forces and means in an efficient way. It is planned to use these forces and means in case situations occur which bear the hallmarks of a crisis. This is a result of withdrawing from the creation of separate plans concerning the protection of critical infrastructure, a change in the definition of critical management and tasks that come within the scope of civil planning. The study that refers to national security threats defines their structure and ways of preparing for them and approving them. The report emphasises the role of the chief of the Internal Security Agency, in the part concerning terrorist threats, and the Director of the Government Centre for Security as a coordinator of the work in its entirety. On 7 September 2010 the Council of Ministers accepted the plans regarding a change in the critical management act, which was submitted by the Minister of Internal Affairs and Administration. The amendment to the act was necessary due to the need for enforcing the Polish law common directive 2008/114/WE concerning identifying and appointing The European Critical Infrastructure and the requirements within the scope of improving its protection. In accordance with the directive, the process of identifying and appointing the European Critical Infrastructure finished in 2011. The Report's contents concerning national security threats is the necessary point of departure from preparation which corresponds to the current needs of the country's National Critical Management Plan and critical managements plans at any level of public administration. The report that refers to threats will serve to ensure cohesion between critical management plans and other plans which have to be fulfilled as a result of other regulations. It will lead to the realisation of planned activities and eliminate duplicate undertakings. According to the author's definitions, the terms mentioned in the text have a fundamental significance for interpreting and applying the act in a way that ensures respect for citizens' rights and freedoms. They are the point of departure to any action which may lead to severe interference in the sphere of an individual's freedom. They are formulated in a way which leaves a margin for interpretative freedom.

The definition of a critical situation emphasises issues concerning severance or significant violation of social ties. It also refers to occurrences described as severe disruption in the functioning of public institutions. It is impossible to claim unambiguously whether the category of public institutions includes only the subjects possessing imperious competences or organisational units which are included in public administration, or even units functioning as private subjects but accomplishing tasks within the scope of public administration. These doubts seem to be impossible to explain on the basis of interpretation. According to the initiator it disturbs the principle of proper legislation. By contrast, the definition of critical infrastructure uses, among other things,: the notion of systems which serve to ensure the efficient functioning of public administration bodies, as well as institutions and enterprises. It is necessary to determine the elements included in critical infrastructure in a detailed and precise way, so that private subjects can unambiguously establish who is obliged to accomplish tasks determined in the act and in what situations. Critical infrastructure means systems and functional objects which are connected with each other, including: building, devices, systems, key services for a country's security and its citizens' security, and other services and objects which deal with ensuring the efficient functioning of public administration bodies as well as institutions and enterprises. Critical infrastructure includes the following systems:

- power and fuel supply;
- communications and computer network;
- financial;
- food and water supply;
- health care;
- transport and communications;
- rescue;
- ensuring continuity in public administration action;
- producing, storing, keeping and using chemical and radioactive substances, including pipelines carrying hazardous substances.

The term critical infrastructure encompasses both public and private sectors[3]. The results of disruptions in different sectors are not limited to the internal

3 Encyklopedia Powszechna, edition. 2, Warszawa 1997, p. 344.

problems of a particular country. National energy systems are connected with each other, in many cases similar to financial and telecommunications systems, mail, or systems concerning air traffic control, which simultaneously are as trans-critical as pipelines, gas pipelines and railway lines. Therefore it is understandable that there is a need for wide cooperation in the field of critical infrastructure, not only in national but also international ranks. In literature on the subject there is a general consensus about the basic meaning of the term *critical infrastructure;* however, the results of the attempts to define it differ from each other. A working definition created by experts from the NATO Civil Protection Committee is as follows: 'critical infrastructure means objects, services and informational systems which are so vital for the country that their damage or destruction would have an impact of no small importance on the country's security, national economy, health, public security and proper functioning of government'. NATO experts claim that the ability to protect is inseparably connected with critical infrastructure. On the basis of the act[4] it determines the way to fulfil duties and cooperation, which are included in the act, within the scope of the National Programme of Critical Infrastructure Protection, hereon referred to as the "Programme", by public administration bodies and services responsible for the security of the nation, proprietors of separate and dependent objects, systems, critical infrastructure devices and services which are "called critical infrastructure operators", and other bodies and public services. The Programme is prepared by the director of the Government Centre for Security, hereon referred to as the centre's Director.

Ministerial directives concerning planning in infrastructure fields

The Plan of critical infrastructure, called the "Plan", is compiled in paper and electronic versions and includes:

General data which must be included in plans sent to superior ranks, particularly:

4 Wider act of management…op. cit. - Article. 5b Act 10, Dz. U. from 2007, No. 89, item 590.

- name and address of dislocation of critical infrastructure;
- numbers: National Official Business Register, Taxpayer Identification Number, National Court Register right for the enterprise of the critical infrastructure's operator;
- data of the person who manages the enterprise on behalf of the critical infrastructure's operator if this person exists;
- data of the person who is responsible for staying in touch with actual subjects that fall within the scope of critical infrastructure;
- name and surname of the person who creates the plan.

Critical infrastructure's data includes:
- shortened description and technical parameters;
- a plan or a map including the localisation of objects and various systems;
- connections with other objects, systems, devices and services.

Description of:
- threats to critical infrastructure and assessment of risk of occurrence with predictable action scenario;
- the correlation between critical infrastructure and other critical infrastructure systems and the possibilities of disrupting its functioning as a result of disruptions which have appeared in interdependent systems of critical infrastructure;
- own knowledge available to be used with the aim of protecting critical infrastructure;
- sources of proper services concerning territory, inspections and guards which can be used with the aim of protecting critical infrastructure.

Variants of:
- action in case of threats or disruptions in critical infrastructure functioning;
- ensuring continuity in critical infrastructure action;
- critical infrastructure reconstruction.

Principles of cooperation with the following competent bodies concerning location:
- centres of critical management;
- inspectorates, guards and services.

The plan is signed by the operator of critical infrastructure or by the person who manages on his behalf and by the person who creates it. The operator of

critical infrastructure has a right to include in the plan other elements which are not mentioned in the Act 1, taking critical infrastructure's specifications and a description of threats into account. Regulations concerning the protection of secret information are applied to the plan because there may be confidential data within the information. As concerns the responsibility for accomplishing tasks in crucial areas, the plan requires agreement within the area which concerns them, with territorial competence of the following:

- the Chiefs of the Internal Security Agency;
- the bodies of the local authority unit;
- the directors of services, inspections and guards.

Agreement is made on the basis of signing an agreement report. It is worth adding that any refusal to agree to the plan requires written justification and indicating the elements which need to be amended or supplemented, as well as supplying a new date for submitting the plan. Refusal to agree the plan, entirely or partly, can occur in the following cases:

- the requirements are not fulfilled, contained in Article 2;
- the presentation of solutions which do not guarantee the security of critical infrastructure;
- a lack of cohesion with the National Programme of Critical Infrastructure Protection, contained in Article 5b of the quoted agreement.

The operator of critical infrastructure, or the person who manages on his behalf, is responsible for the accomplishment of the agreed plan. Revision of the plan is a functional process. The operator of critical infrastructure who is in possession of the other plan, worked out on the basis of separate regulations and requirements, can submit the plan to the director of the Centre. The aim is to accept that the duty of possessing a particular plan meets the requirements of the plan of critical infrastructure if fulfilled. Suitable coordination of interdepartmental work is necessary, with particular consideration for structures which are substantially suitable and subordinate to particular departments, including: The Agency of Material Reserves, the Major Sanitary Inspectorate, the Major Veterinary Inspectorate, The Major Inspectorate of Environmental Protection, the Major National Fire Brigade Headquarters, the Major Police Headquarters, the Major Headquarters of the Border Guards, the Major Headquarters of Military Police, the Government Agency for Security, the Polish Airports State Enterprise, the

Polish State Railways, the Polish Agency of Atomism, the Polish Postal Service, Polish Petroleum and Gas Mining, the High Mining Office, the Electronic Communications Office, the Energetic Control Office, the General Directorate of State Roads and Motorways and the Civil Aviation Authority. Participation of the Minister of Infrastructure is required in particular undertakings concerning critical infrastructure.

Analysis of the documents and the current action being taken by European Countries leads to decision making concerning working out of the so-called *Green Book*, which presents the possibilities for action in the European Programme for Critical Infrastructure Protection (EPCIP). The main aim of *The Green Book* is to obtain information concerning possible options of politics on the basis of the involvement of a large number of interested parties. The aim of the Programme is to ensure the existence of suitable and identical levels of protective security within the scope of critical infrastructure, limiting the damage to a minimum and providing fast and proven means of repair in the entire European Union. Currently, in Europe, there are cyclical meetings or seminars concerning issues of critical infrastructure protection. Representatives of the Major Headquarters of the National Fire Brigade and the Minister of Economy and Work take part in the meetings that have been already mentioned and are usually devoted to the problem of the entire critical infrastructure, including the cooperation of public administration with the private sector. It is worth adding that this cooperation is treated as a priority. This is caused by the fact that, in many cases, owners and operators of particular units are responsible for critical infrastructure protection. A common document concerning EPCIP was presented during one of the seminars. In the document the following task areas were identified:

- ensuring public order
- ensuring security
- managing the judiciary prison system
- ensuring law and public order
- diplomatic communications
- ensuring law and public order
- spreading governmental information
- the armed forces
- civil administration
- road transport

- rail transport
- air transport
- inland transport
- sea transport
- pipelines control
- transport, production, storing and processing chemical and nuclear substances
- transport of hazardous goods (chemical and nuclear substances) by all means of transport, including pipelines.

Because the problem of critical infrastructure goes beyond the scope of competence of particular departments, the institution was identified as being responsible for the coordination of interdepartmental cooperation, as well as coordination of cooperation with KE within that scope. The Ministry of Internal Affairs took up the function of coordinator of the problem of protecting critical energetic infrastructure against any destructive action, particularly against terrorist attacks.

Analysing all the documents which concentrate on security, the author of this paper has matched the study done by the Ministry of Defence Affairs Department of Infrastructure with the participation of other organisational sections, which come under or are supervised by the Infrastructure Ministry, which presented several significant tasks. Ensuring suitable levels of critical infrastructure's security, minimising its weak points, as well as making fast and proven plans concerning reconstruction, are the proper aim of EPCIP, which takes into account all threats referring to the priority of terrorism. This is an elastic approach because, apart from terrorism, other kinds of threats with similar aims are taken into account. Enumerated principles are crucial as well and should be the basis of EPCIP. What is more, another principle concerning equal rights for countries taking part in the Programme should be added to them. Extension of critical infrastructure, as well as its protection of one country, should not be harmful for the business of other people or countries. Arranging the so-called common scope of EPCIP is and will be helpful in determining: the responsibility of countries which show their interest, the group of obligations which will be compulsory, and the group of voluntary obligations.

It should be remembered that our country is not a green island – there are examples that can be taken from events in Lithuania. Therefore, the most prominent watchwords of Critical Infrastructure are the following: physical reserves, services, computer equipment, networks and other elements of infrastructure, whose disruption or damage would have a severe influence on health, security, economic or social prosperity with reference to three or more membership countries. The result is that the conceptions worked out by the operators of protection plans, concerning objects counted among critical infrastructure, should be implemented whereever possible. The plans mentioned above ensure cohesion of action for the security of one or many countries of united Europe. Owners and operators should have the following rights: reporting a suitable body if particular infrastructure has a critical nature, participation in devising a plan of action against threats to critical infrastructure together with suitable civil defence bodies and law enforcement bodies of membership organisations, and the opportunity to apply for the refinancing costs incurred from the Budget or the European Union.

The following issues are taken into account: organising dialogue with the owners and operators of critical infrastructure at national and European level on the basis of creating platforms concerning information exchange and views regarding its protection. The level of information exchange should be made conditional on the problems' significance and accounted for amongst national or European critical infrastructure.

The Net of Early Warning about a Threat to Critical Infrastructure should take electronic form and be based on modern technologies concerning information transfer. The resistance of the net should be as great as possible. National segments should be organised by each country separately. The International sector – European Union - should announce the coordinators of critical infrastructure. It is possible to develop trade nets as well.

National Programme for the Protection of Critical Infrastructure

The Government Centre for Security is responsible for preparing the National Programme of Critical Infrastructure. While preparing the Programme, the Centre cooperates with ministers and directors of central offices competent in issues of national security and responsible for the systems of critical infrastructure. The Programme mentioned in this paragraph describes:

- national priorities, aims, requirements and standards destined to ensure efficient functioning of critical infrastructure;
- ministers who manage the actions of government administration and the directors of central offices responsible for the systems mentioned above;
- detailed criteria which lets us distinguish objects, systems, devices and services which are a part of critical infrastructure systems, taking into account their significance for the functioning of the country and the fulfilling of citizens' needs[5].

Regulations which were proposed by Minister of State Treasury on 18 November 2009 ensure the government influences the management of property including: objects, systems, devices and services which are a part of the so-called critical infrastructure in the energy sector, which has a particular significance for the power security of the country. The act provides for the particular rights of the minister who is competent in referring to the issues of the State Treasury and their accomplishment in some capital partnerships or capital groups which carry out activity concerning the electric energy, petroleum, and gas fuel sectors. New regulations will include, within their scope, partnerships which carry out their activity in the following sectors: electric energy, petroleum and fuel partnerships. In companies which manage critical infrastructure it will be possible to put forward an objection to the decisions taken by the authorities of the partnership. The objection of the Minister of State Treasury may concern the resolution adopted by the board of directors of the partnership concerning the following issues: dissolution of the partnership, change of purpose, selling or leasing the enterprise and abandoning the exploitation of elements of property.

5 www. reg.gov.pl.infrastruktura/dokumenty 2009 r.- Government Centre of Security.

An objection may be expressed towards accepting a material and financial plan or a long-standing strategic plan of the partnership. In accordance with the act's regulations, the director of the Government Security Centre accomplishes his duty by making a list of elements concerning critical infrastructure in the energy sector, which includes: objects, systems, devices and services devoted to the power and fuel supply. In the electric energy sector this is the infrastructure connected with manufacturing and industry,; in the petroleum sector it is the infrastructure connected with extracting, refining, processing, storing, transporting by pipelines and port terminals to handling, and in the sector of gas-fuels – objects referring to producing, extracting, refining, transporting and terminals for liquefied natural gas. Regulations which tell us about security and responding to critical situations introduce the function of a liaison office worker to the issues concerning protection of critical infrastructure. This person is appointed by the partnership with the State Treasury Minister's and Government Security Director's approval. The liaison office worker must monitor the activity of the partnership within the scope of activities it carries out, particularly referring to decisions regarding the management of the elements of its possessions. The worker's task is to prepare a report about the state of the protection of critical infrastructure, referring to the particular institution. The report is handed over to the Minister of State Treasury and the Director of the Government Security Centre. Then it is analysed and motions are returned to the interested parties. The duty to determine the list of partnerships (The State Treasury has particular rights here) in a government order was abolished. The objects of critical infrastructure must be marked and placed in a uniform list made available to the interested parties that have rights to it. It is expected that the list mentioned above will include all the partnerships referring to critical infrastructure regardless of their property type. To date there has not been an act regarding these registers and lists. New legislation within the scope of critical management allows us to adapt Polish legislation to common legislation repealing the act from 3 June 2005 of the particular rights of the State Treasury and their use in capital partnerships, which is of great importance for public order and protection of the country's critical infrastructure. Regional Programmes for protection of critical infrastructure are also changed and adapted to the programmes of the European Union[6].

6 „Gazeta Podatnika" everyday bulletin No. 232 from the 07th December 2009.

Poland's Critical Infrastructure, which has an influence on European Infrastructure as a whole, includes the following: physical sources, services, computer equipment, nets and other infrastructure elements whose disruption and damage would have a severe effect on the health, security, economic and social prosperity of three or more membership countries. The concept worked out by the operators of protection plans counted among critical infrastructure would be analysed and accepted by the body which coordinates the protection of critical infrastructure in a particular country. The financial consequences for operators who do not carry out tasks aimed at accomplishing a protection plan should be also considered. The plans mentioned above should ensure cohesion of action for security and the owners and operators of critical infrastructure in all countries of the European Union should have the right to report to a suitable body that a particular infrastructure may have a critical nature. What is more, participation in devising a plan of action to deal with threats connected with critical infrastructure should make it possible to apply for refinancing costs incurred from the Budget or the European Union.

The following issues are taken into account: organising dialogue with the owners and operators of critical infrastructure at national and European level on the basis of creating platforms concerning information exchange and views regarding its protection. The level of information exchange should be made conditional on the problems' significance and accounted for amongst national or European critical infrastructure.

The Net of Early Warning about the Threat to Critical Infrastructure should take electronic form, based on modern technologies concerning the spread of information. The resistance of the net should be as great as possible. National segments should be organised by each country individually. The International sector of the European Union's action should be referred to the national coordinators of critical infrastructure, because it is possible to develop trade nets as well.

The telecommunications sector, together with the energy department, decides on the functioning of the majority of other sectors. For the vast majority of sectors, not to say all of them, reliable access to telecommunications services is an issue of great importance. Society's dependency on the functioning of permanent and proper telecommunications means that ensuring the telecommunications network

and its services are resistant to damage and interference, as well as present threats to the telecommunications structure, acquires the greatest importance.

Possessing a strategy which ensures maintaining the necessary level of security and preparing plans concerning the functioning of telecommunications during particularly threatening situations is also a significant issue.

The Council of Ministers has accepted the National Programme for the protection of Critical Infrastructure, hereon called *the Programme*, whose aim is to create conditions for improving the security of critical infrastructure, particularly within the scope of the following issues:

- preventing disruption in the functioning of critical infrastructure;
- preparing for critical situations which can affect critical infrastructure;
- responding to situations concerning disruption in the functioning of critical infrastructure;
- reconstructing critical infrastructure.

The Programme, which consists of the issues mentioned above, determines unambiguously:

- national priorities, aims, requirements and standards destined to ensure efficient functioning of critical infrastructure;
- ministers who manage action of government administration and directors of central offices responsible for systems which are included in the act;
- detailed criteria which lets us distinguish objects, systems, devices and services which are a part of critical infrastructure systems, taking into account their significance for the functioning of the country and fulfilling citizens needs.

The Programme presented in three parts is a general and schematic one. It is accomplished by people responsible for systems referring to Article 3, Point 2 in the Directive of the Council of the European Union[7].

7 Council's Order 2008/114WE …, op. cit., Article. 3.

Summary

The issues presented and the part, or the particular element, of the Programme show how it all contributes to supporting the efforts of member states whose aims are: preventing terrorist attacks and other events referring to internal security, preparing for such attacks or events, protecting people and critical infrastructure against terrorist attacks and other events connected with national security. The Programme should contribute to ensuring protection in the following fields: critical management, environment, public health, transport, research and technological development, as well as economic and social cohesion, areas of terrorism and other kinds of security risks as part of freedom, security and justice. One of the key elements ensuring efficient and overall protection of critical infrastructure is the cooperation of public sector with the private sector, as well as cooperation within these sectors, paying particular regard to cooperation between representatives of particular systems in the private sector.

The significant element of cooperation is working out clear principles and procedures between two parties: bodies and state services and the second party: owners of self-contained and dependent objects, systems and devices of critical infrastructure. This results from the fact that a major part of infrastructure, which has a crucial meaning for a country's security, is in the private sector's hands. In order to do this, the cooperation of public and private sectors comes down to the following issues: transferring and exchanging information, establishing channels of information for alarm signals which come from state services, as well as responsibility and ensuring the security of the data, which constitutes the confidentiality of commerce received from operators.

References

Administration towards critical situations, Material from the conference at the School of Public Administration, 6–8 May 1998.

Article 26 Act. 4, The act about critical management op. cit. Dz. U. from 2007, No. 89, item 590 and (FinansePublU). Dz.U. from 2007, No. 249, item 2104 with further changes.

Article 137 act from 21 November 1967 about the common duty of the defence of the Republic of Poland, uniform text, Dz. U. from the 2004, No. 241, item.2416 with further changes

Article 4 of Alliance

Balcerowicz B, *Wybrane problemy obronności państwa*, AON, Warszawa 1997.

Bezpieczna Europa w lepszym świecie: Europejska Strategia Bezpieczeństwa, Bruksela 12th December 2003

Białas A, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie,* Wydawnictwo Naukowo-Techniczne 2006.

Directive of the Council, 2008/114/WE from the 18t December 2008, Dz. U. U. E. from 2008, No. L 345/75.

Forowicz K, Freonowa paranoja. Rzeczpospolita from 8 August 2007 Temperatura rozmów o temperaturze, Rzeczpospolita from 10 October 2007 r. Miliony dolarów na środowisko, Rzeczpospolita from 30 October 2007

Grzywna A., Regional economic integration on the Iberian Peninsula, the master's dissertation written at the Department of International Relations at Karol Adamiecki University of Economics in Katowice, supervised by prof. PhD. T. Sporka, Katowice 2009.

Grzywna, A., *Wpływ Azji na kształt międzynarodowego bezpieczeństwa i gospodarkę, Funkcjonowanie podmiotów gospodarczych w warunkach niepewności*, eds. A. Limański, R. Milic-Czerniak, WSZMiJO, Katowice 2010, pp. 37-45.

Grzywna Z, *Koncepcja wykorzystania zasobów w sytuacjach niemilitarnych zagrożeń w województwie Śląskim*, AON, Warszawa 2004.

Grzywna Z, *Przygotowanie oddziałów pozamilitarnych do działań w sytuacjach kryzysowych na przykładzie Śląska*, AON, Warszawa 2000.

http.//Infrastruktura_krytyczna#regionalne_programy_ochrony_infrastruktury_krytycznej.

Kamieniecki, W., *Wykorzystanie systemów wieloagentowych do poprawy bezpieczeństwa informatycznego przedsiębiorstw z wykorzystaniem urządzeń Vyatta, Funkcjonowanie podmiotów gospodarczych w warunkach niepewności*, eds. A. Limański, R. Milic--Czerniak, WSZMiJO, Katowice 2010, pp. 215-222.

Kitler W. B. Wiśniewski, J. Prońko, *Wybrane problemy zarządzania kryzysowego w państwie*, AON, Warszawa 2000.

Kitler W., *Wybrane aspekty kierowania państwem w sytuacjach kryzysowych w obronie narodowej RP wobec wyzwań i zagrożeń współczesności*, AON, Warszawa 1999.

Strategic conception from 1991, vide: NATO, „Review" No. 6 from 1991, p. 2. Section 25 or.

Konieczny J., Ratownictwo w systemie bezpieczeństwa publicznego, Gramond, Poznań, 2002.

Constitution of the Republic of Poland, from 2 April 1997, http://edu/library/poland/konst.

Constitution of the Republic of Poland, Dz. U. from 1997, No. 78 item. 483. with changes.

Convention on protection of world cultural and natural heritage, accepted in Paris, on 16 November 1972, Dz. U. from 1976, No. 32, item. 190 and 191.
Korycki S., *System bezpieczeństwa Polski*, AON, Warszawa 1994.
Koziej S., *Rozważania o przyszłej strategii NATO oraz strategii bezpieczeństwa i obronności Rzeczypospolitej Polskiej*, AON, Warszawa 1999.
Koziej S., *Strategia i potencjał obronny Polski w warunkach członkostwa w NATO*, AON, Warszawa 2001.
Krzyżanowski L., *Podstawy nauk o organizacji i zarządzaniu*, PWN, Warszawa1998.
Declaration of the Speaker of the Sejm of the Republic of Poland on 15 May 2009 concerning announcing the uniform text of the act on the principles of development policy Dz. U. from 2009, No. 84 item 712.
Ochrona ludności. Wybrane zagadnienia, Firex", Warszawa 1997.
Palme, Commission's Final Statement, A World at Peace-Common Security in the Twenty First Century, "New Perspectives"1989 r. Nr 6.
Telecommunications Law (Dz. U. from 2001, No. 73, item. 852, from 2002, No. 122, item 1321 and No. 154, item 1800 and 1802, No. 25, item 253, No. 74, item 676 and No. 166, item 1360 and Dz. U. from 2003, No. 50, item 424 and No. 113, item 1070, No. 130, item 1188 and No. 170, item 1652).
Project from 4 December 2008 referring to the change of the act of critical management Dz. U. from 2008 No. 89.
Chapter 3 of Constitution of the Republic of Poland, Dz. U. from 1997, No. 78. item 483.
National Defence Minister's Order from 14 June 2004 concerning the records of military services for defence, Dz. U. from 2004 No. 148, item.1556.
Government Order from 11 August 2004 concerning personal and material benefits for defence in the event of an announcement of mobilisation and war Dz. U. from 2004 No. 203 item 2081.
Government Order from 3 August 2004 concerning material benefits for defence during peace Dz. U. from 2004 No. 181, item1872.
Government Order from 6 January 1998 Dz. U. from 2004 No. 5, item.15. with changes.
Strategy of the national security of Poland was accepted on 13 November 2007 by the President on the Prime Minister's motion. The document was published on the basis of the article 4a point 1, section 1 of the act from 21 November 1967 r. of common duty referring to the defence of the Republic of Poland.
The text accepted by the European Parliament on 22 April 2009 r Procedure 20080/2000 CNS text A6/0228.
Tarnawski M., *Wspólna Polityka Zagraniczna i Bezpieczeństwa* – rzeczywistość czy fikcja?, „Zeszyty naukowe Zakładu Europeistyki Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie", eds. A. Jurkowska, M. Szewczyk, No. 2(7) 2008 r. Szkice z dziedzin nauki, Rzeszów 2008.
Tyrała P., *Sekuritologia. Bezpieczeństwo kompleksowe*, Rzeszów 2010.

Urban A., *Bezpieczeństwo społeczności lokalnych*. Wydawnictwa Akademickie i Profesjonalne (WAiP). Warszawa 2009.

The act of the common duty of defence Article 17.RP. Dz. U. from 2004 No. 241 item., 2416 which is subject to change

The act of common duty referring to the national defence of the Republic of Poland Dz. U. from 2004 No. 241, item. 2416. with changes. and orders op. cit. from 25 June 2002 referring to the scope of action of the Chief OC. Dz. U z 2002 r. Nr 96, poz. 850.

The act of the state of natural disaster , Dz. U. from 2002 No. 74, item. 676, from 2006 No. 50, item 360 and No. 191, item. 1410, from 2007 No. 89, item. 590 and from 2009 No. 11, item. 59.

The act detailing the act's changes concerning critical management Dz. U. from 2004 No. 131 item. 1076.

The act from 5 June 1998. No. 91 item. 576 with further changes, it is about planning and creating solutions concerning infrastructure, the acts were announced in Dz. U. z 2001 No. 142, item. 1590, with further changes about planning and creating solutions referring to infrastructure which improves the level of the security of people during threats, it concerns the public security and protection of people, Dz. U. from 2002 No. 23, item. 220, No. 62, item.558, No. 214, item. 1806 i No. 153, item 1271, from 2003 r. item.162, item. 1568, from 2004 No. 102, item. 1055, No. 116, item. 1206, from 2006 No. 126, item. 875 and No. 227, item. 1658, from 2007 No. 173, item. 1218, from 2008 No. 180, item. 1111, No. 216, item. 1370 and No. 223, item. 1458.

The act from 21 June 1996 about the Office of the Minister of Internal Affairs and Administration. Dz. U. from 1996 No. 106, item 491. with further changes, but this is not specified completely. In a further part of the text there will be a reference to new acts.

The act from 21 November 1967 about the common duty of defence Dz. U from 2004 No. 241, item 2416.

The act from 21 November 1967 about the common duty of the defence of the Republic of Poland Dz. U. from 2004 No. 241, item 2416, with changes.; The act from 24 October 2008 about the change of the act of the common duty of the defence of the Republic of Poland and the act of military service of regular soldiers Dz. U. from 2008 No. 206, item 1288.

The act from 4 September 1997 about government administration's sections Dz. U. from 1997 No. 141, item 943, with changes. Article 15 of the act from 5 June 1998 about government administration in the province, Dz. U. from 1998 No. 91, item. 577, with changes and Article 4 of the act from 5 June 1998 r. about county self-government in Dz. U. from 1998 No. 91, item 578.

The act from 5 June 1998 about self-government of the county Dz. U. from 2001 No. 142, item. 1592, with further changes referring to efficient fire defence and preventing other special threats of life, health, people and environment.

The act from 6 December 2006 of the principles of run development policy Dz. U. from 2006 No. 227, item. 1658 with further changes published in Dz. U. from 2009 No. 84, item. 712.

The act from 8 March 1990 of the self-government district Dz. U. from 2001 No. 142, tem. 1591, with changes

The act from 21 November 1967 of the common duty of the defence of Poland, uniform text, Dz. U. from 2004 No. 241, item. 2416 with changes.

Walentek A., Common security, conversation with general F. Dela, contemporary Chief of National Civil Defence, „Dziennik Polski" 1998, No. 162.

Wojciechowicz W., *Ochrona infrastruktury krytycznej państwa*. AON, Warszawa 2004.

www.rcg.gov.pl.infrastruktura/dokumenty 2009 - Government Security Centre

Zalewski S., Unia Europejska jako wspólnota bezpieczeństwa, „Kształcenie obywatelskie w wojsku", part 2, MON, Warszawa 2002.

Zieliński J., Bezpieczeństwo wewnętrzne wobec globalizacji, in: Problemy bezpieczeństwa wewnętrznego i bezpieczeństwa międzynarodowego, edited by K. M. Księżopolskiego, Wyższa Szkoła Administracyjno-Społeczna, Warszawa 2009.

Zieliński J., Bezpieczeństwo wewnętrzne wobec globalizacji, w: Problemy bezpieczeństwa wewnętrznego i bezpieczeństwa międzynarodowego, edited by Krzysztofa M. Księżopolskiego, Wyższa Szkoła Administracyjno-Społeczna, Warszawa 2009..

Zięba R., *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych, Fundacja Stosunków Międzynarodowych*, Warszawa 1998.

Changes in the uniform text (concerning equipping the warehouses with rescue equipment) of the act mentioned were announced in Dz. U. from 2002 No. 23, item. 220, No. 62, item. 558, No. 113, item. 98item. 1568, from 2004 No. 102, item. 1055, No. 116, item. 1203, from 2005 No. 172, item. 1441, No. 175, item. 1457, from 2006 r. No. 17, item. 128 i No. 181, item. 1337, from 2007 No. 48, item. 327, No. 138, item. 974 i No 173, item. 1218, from 2008 No. 180, item. 1111 and No. 223, item. 1458 and from 2009 No 52, item. 420.