Title: System and Human Safety: Critical Infrastructure and Anti-Terrorist Attachment

Author: Karolina Wojtasik, Marek Grochowski, Vit Horák

Citation style: Wojtasik Karolina, Grochowski Marek, Horák Vit. (2019). System and Human Safety: Critical Infrastructure and Anti-Terrorist Attachment. “System Safety: Human - Technical Facility – Environment” (Vol. 1, iss. 1 (2019), s. 894-901), doi 10.2478/czoto-2019-0114

sciendo CzOTO 2019, volume 1, issue 1, pp. 894-901

SYSTEM AND HUMAN SAFETY: CRITICAL INFRASTRUCTURE AND ANTI-TERRORIST ATTACHMENT

doi: 10.2478/czoto-2019-0114
Date of submission of the article to the Editor: 29/11/2018
Date of acceptance of the article by the Editor: 0401/2019

Karolina Wojtasik[1] – *orcid id: 0000-0002-1215-5005*
Marek Grochowski[2] – *orcid id: 0000-0002-8085-0632*
Vit Horák[3] – *orcid id: 0000-0003-2596-0975*
[1] University of Silesia – **Poland,** *karolina.wojtasik@gmail.com*
[2] Zakłady Mechaniczne „BUMAR – ŁABĘDY" S.A., Ośrodek Badawczo-Rozwojowy Urządzeń Mechanicznych „OBRUM" sp. z. o. o. – **Poland**
[3]University of Ostrava – **Czech Republic**

Abstract: The critical infrastructure (CI) has an important place in Polish security system. The article discusses legal acts and characterises the notion of critical infrastructure as an element essential for the functioning of the society. As a result of the entry into force of the Anti-terrorism Act from 10 June 2016 (Journal of Laws [Dz. U.], item 904), the current procedure of security plan acceptance was extended to include participation of the Internal Security Agency through the requirement to submit a so-called anti-terrorist attachment. The article is an analysis of the constituent parts of the document and procedures it covers. Moreover, the authors present conclusions and recommendations resulting from the analysis of AT attachments of CI facilities and other facilities subject to mandatory protection. The empirical system of reference is based on facilities located in Silesia. The authors described their experiences related to the process of preparation and acceptance of AT attachments as well as conclusions based on employee trainings conducted in workplaces where anti-terrorism procedures are in force.
Keywords: critical infrastructure (CI), mandatory protection, crisis management, anti-terrorism, anti-terrorist attachment

1. INTRODUCTION

The aim of the article is to analyse the functionality of *security plan related to facilities and equipment subject to mandatory protection in respect of terrorist threats*, i.e. the so-called anti-terrorist attachment (AT attachment). The empirical system of reference of this article is based on facilities located in Silesia (some of them constitute the so-called critical infrastructure - CI) which are subject to mandatory protection. The theoretical system of reference is based on the issues regarding security culture and sociology of work. The article explains key notions: critical infrastructure, mandatory protection and anti-terrorist attachment. The analysis of 14 anti-terrorist attachments

allowed to assess functionality of the solutions and to develop recommendations regarding the current procedure.

2. THEORETICAL SYSTEMS OF REFERENCE

Workplace is a social system which is an integral component of a wider economic, political and cultural system. The element which bonds this social system together is the organisational culture developed more or less consciously by employees (Suchacka, 2017). Scientific reflection on the organisational culture draws predominantly from organisational sociology but also from social psychology, sociology of work and anthropology. Organisational culture of a company consists of social norms, value systems stimulating the employees, organisational climate, way of management, shared meanings and symbols, cognitive schemas and rules of conduct (Nogalski 1998:105). In addition, it is a system of though and behaviour patterns which are established within social environment of a given organisation and have impact on the achievement of its formal objectives (Sikorski, 2012). Organisational culture is defined either as a pattern of fundamental assumptions, discovered or developed by a given group through the process of learning, external adaptation and internal integration or as a pattern of values, frequently perceived as self-evident, which help members of an organisation to understand which actions are acceptable and which are not. Technical culture – an attitude toward technical devices utilised within a workplace is also an element of organisational culture (Ejdys, 2010). Another noteworthy notion is the security culture of an organisation which is a state of threat awareness of the employees, formal and informal norms of response to dangerous situations as well as technical and organisational preparations which affect the level of attention for security and health protection in managing a company, organizing tasks, supervising and assessment of the employees (Ejdys, 2010). In this respect, the introduction of the obligation to prepare the anti-terrorist attachment is a very important step in developing and strengthening the security culture of workplaces essential for the functioning of the Republic of Poland and Polish society. Actions undertaken to provide an adequate protection of the country's critical infrastructure are a significant step towards building a civil society which is aware of dangers, able to counteract them and, in a crisis situation, react to them.

3. CRITICAL INFRASTRUCTURE OF A STATE

According to the Crisis Management Act of 26 April 2007 (Journal of Laws [Dz. U.] from 2013 item 1166 and from 2015 item 1485), critical infrastructure consists of *systems and its constituent functional facilities, including structures, equipment, installations, services which are crucial to the security of a state and its people and which ensure the effective functioning of public administration, institutions and businesses*. *Critical infrastructure includes systems related to: energy supply, energy-producing raw materials and fuels, communications, IT networks, finance, food and water supply, health protection, transport, medical emergency response, continuity of public administration, production, holding, storage and use of chemical and radioactive substances including pipelines for dangerous substances*. CI consists of physical and software systems (facilities, equipment and installations) necessary for basic functioning of the economy and country. Not every strategic facility is a part of critical infrastructure. The decision of inclusion of a given facility in the CI is based on

detailed criteria specified in a classified attachment to the *National Programme for Critical Infrastructure Protection (2018)*.

CI facilities play a crucial role in the proper functioning of a state and the life of society. However, critical infrastructure is susceptible to destruction, damage and disruption, which may be caused by forces of nature or human actions, entailing threat to life and property of citizens as well as negative consequences to the development of the economy. It is impossible not the mention the psychological effects – fear, sense of insecurity in society and lack of trust in all levels of government. Therefore, it is one of the top priorities of the authorities of the Republic of Poland to protect critical infrastructure through, according to the article 3, point 3 of the Crisis Management Act, *all actions designed to ensure functionality, continuity of operation and integrity of critical infrastructure in order to prevent threats, risks or vulnerabilities, limit and neutralise their effects and quickly restore the infrastructure in case of a failure, attack or other event interfering with its proper functioning.* As reflected on the website of the Polish Government Centre for Security (Rządowe Centrum Bezpieczeństwa): "One of the elements of crisis management related to critical infrastructure protection is the cooperation of public administration. The cooperation consists in joint actions designed to improve safety conditions. Another important element is the cooperation between the administration and business. Its aim is to develop transparent rules and procedures by both the administration and sole or dependent owners of structures, installations or equipment categorised as part of critical infrastructure. This is due to the fact that a substantial part of the infrastructure of key importance for national security is currently in the hands of private sector" (https://rcb.gov.pl/zarzadzanie-kryzysowe/).

It should be noted that special services perform a specific role in CI protection. These agencies have at their disposal well-trained personnel and resources for identification of threats caused by intentional human action. Sharing information related to threats with CI operators and other entities competent in the field of CI protection is crucial to planning the security of these structures and assessing the risk of an attack. A special role is played by the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego). According to the article 4, sections 1-3 of the Anti-Terrorism Act: Public administration authorities, owners and holders of structures, installations, equipment of the public administration or critical infrastructure cooperate with bodies, agencies and institutions competent in the field of security and crisis management in the implementation of anti-terrorist activities. The abovementioned bodies and entities immediately inform the head of the Internal Security Agency about terrorist threats to public administration infrastructure or critical infrastructure including threats to systems and networks related to electric power, water and sewage, heating and IT which are important from the point of view of national security. When information on possibility of a terrorist action threatening public administration infrastructure or critical infrastructure, life or human health, property, national heritage or environment reaches the agency, the head of the agency can issue instructions to the bodies and entities in danger providing them with necessary information on how to counter, eliminate or minimise the impact of the threat. Additionally, these bodies and entities report to the head of Internal Security Agency on the actions taken in that respect.

4. ANTI-TERRORIST ATTACHMENT TO SECURITY PLAN

According to the legal definition, mandatory protection means: protection of areas, structures, equipment and shipments crucial to the defence and economic interest of the country, public security and other important interests of the country provided by specialist armed units or adequate technical protection, in accordance with the relevant provisions of the People and Property Protection Act from 22 August 1997 (Journal of Laws [Dz. U.] from 2014, item 1099 and from 2015, item 1505). Article 5 of the said act divides areas, structures and equipment into groups according to the following categories: national defence, protection of the economic interest of the country, public security, protection of other important interests of the country and additionally: structures (including buildings), equipment, installations, services included in the uniform list of structures, installations, equipment and services which are part of the critical infrastructure. Detailed lists of areas, structures and equipment are prepared by: the President of the National Bank of Poland, National Broadcasting Council, ministers, heads of central offices and governors with respect to subordinated or supervised organisational offices. Inclusion of a given area, structure or equipment in this list is made by means of an administrative decision. Governors keep record of areas, structures and equipment subject to mandatory protection located within a province. According to the data provided by the Police Headquarters (Komenda Główna Policji), within the territory of the Republic of Poland there are 3490 structures subject to mandatory protection (situation at 31 December 2017), of which 368 are located in the Silesian province and an equal number in the Greater Poland province which is the highest number in the country.

Prior to the entry into force of the Anti-Terrorism Act, the acceptance procedure of a security plan of areas, structures and equipment present on the provincial list of areas, structures and equipment subject to mandatory protection consisted in obtaining approval of such plans from the Police Headquarters and Provincial Fire Service Headquarter (Komenda Wojewódzka Straży Pożarnej). According to the current regulations, the preparation of a security plan requires also participation of the Internal Security Agency (in respect of terrorist threats). A result of the entry into force the Anti-terrorism Act from 10 June 2016 (Journal of Laws [Dz. U.], item 904) was the amendment of the article 7, section 1 of the People and Property Protection Act which reads as follows: ”An infrastructure administrator who directly manages areas, structures an equipment present on the list described in the article 5, section 5 or a person authorised by the administrator are obliged to receive acceptance of the security plan of the areas, structures and equipment from the competent provincial Chief of the Police and, regarding terrorist threats, from the competent director of Internal Security Agency local office”. It follows that an administrator of a structure (area or equipment) present on the confidential provincial list of areas, structures and equipment subject to mandatory protection is obliged to prepare and submit to the correct division of the Internal Security Agency the so-called anti-terrorist attachment, i.e. protection scheme of a structure (area or equipment) in respect of terrorist threats. *The acceptance procedure of a security plan of an area, structure of equipment subject to mandatory protection against terrorist threats* available on the Internal Security Agency’s webpage specifies that an AT attachment should consists of: first page form, table of contents with page numbers, table with terrorist attack risk assessment (with risk level to a given area, structure or equipment), personnel evacuation procedure in case of a terrorist threat which takes into account the nature

of the attack (attack using firearms and sharp tools; attack using explosives; chemical, biological, radiological and nuclear attack), the scope of actions undertaken on each state of alert (does not include the CRP states of alert) stipulated in the Anti-terrorist Act (ALFA, BRAVO, CHARLIE, DELTA) in an administrative area where the area, structure or equipment subject to mandatory protection is situated and contact information necessary for mutual cooperation: the address of a facility (structure, area or equipment), fixed telephone number and e-mail address. When the consultations and preparation is performed by a person appointed by the facility administrator, it is necessary to issue an authorisation. AT attachment is a non-classified document. Receiving acceptance takes place as follows: a draft of the AT attachment is prepared and submitted to the competent local office of the Internal Security Agency; if necessary, the director makes required adjustments; 2 paper copies of the AT attachment are submitted to the Internal Security Agency local office which then either accepts the AT attachment or rejects it and sends the 2 copies of the document back with appropriate annotations. Subsequently, the Internal Security Agency local office informs the competent provincial chief of the police (or the Commander-in-Chief of the Police) that the attachment was accepted or rejected. The procedure in its present version has been in force since 1st January 2017 and during the period from January to November 2017 450 attachments has been accepted (of which 200 were pending acceptance). In the following year (situation at 19th November 2018), 1160 AT attachments have been accepted and 180 were pending acceptance..

5. AT ATTACHMENT – STUDY ASSUMPTIONS

The empirical system of reference of this article is based on companies which are known to the authors. However, revealing more detailed information like their names, industry and characteristics is not crucial for the clarity of reasoning and may result in violation of the law. The authors participated in the process of preparation and acceptance of the AT attachments for those facilities. The analysis included in total 14 AT attachments to security plans of businesses subject to mandatory protection, 5 of which were part of critical infrastructure. Both in the case of CI and other facilities subject to mandatory protection, the procedure of acceptance and the contents of the AT attachments is identical. The analysed facilities differed in terms of production specifics, size of the occupied area, number of buildings/equipment situated in the facility, number of employees and the number of specialised security and protection (SUFO/WSO) employees. Although each facility was a separate case, the AT attachments were prepared following the same guidelines. Additionally, the AT procedure training schemes for the personnel of the facilities were analysed as well as reactions and comments made by the employees on the preparation and implementation of procedures in case of a terrorist attack on their workplace. As a result of data analysis, conclusions and recommendations regarding the AT attachment acceptance procedure were formulated. The AT procedure training has not yet been conducted in the study group of facilities, however, it is planned and will be analysed by the authors during next stages of the research process.

6. AT ATTACHMENT IN CI FACILITIES – CONCLUSIONS AND RECOMMENDATIONS

Firstly, the AT attachment is prepared for facilities of very different categories – large industrial plants employing several thousand people or small establishments recorded on the provincial list employing 2-4 people (where during some shifts there is only one person on duty). This requires completely distinct assumptions regarding the procedure for notifying, evacuation and decision-making. In case of a threat, it is impossible to follow the standard procedure for notifying the facility administrator responsible for initiating the evacuation who is in a building situated a couple or a dozen kilometres away. If there is only one specialised security and protection employee (WSO/SUFO) present at all times in such facility and s/he is currently performing a foot patrol on a relatively large area s/he will not be able to evacuate the facility, especially when the situation develops dynamically. The abovementioned conditions make it necessary to train in detail the employees of such facilities with regard to the correct behaviour and procedures related to evacuation for different kinds of threats. The AT attachment is a document which defines these behaviours and materials available at antyterroryzm.gov.pl webpage allow to adequately train personnel.

Secondly, in the acceptance procedure of the AT attachment there are no clear guidelines on the evacuation of personnel crucial for the proper functioning of the production systems, for example people who control technological processes. Disruption of operation of some machines may result in an ecological crisis, endangering of thousands of human lives or substantial economic losses.

Thirdly, the procedure of AT attachment acceptance imposes designation of so-called emergency safe rooms and alternative emergency safe rooms within and beyond a workplace area. In the case of the so-called internal emergency safe rooms it would be ideal to designate a room which is spacious enough for all personnel, has reinforced door, does not have windows (protection against attackers armed with firearms), has water and telephone connections. Finding such room in a production plant proves to be difficult and oftentimes requires an overhaul or infrastructure adjustment. Due to lack of precise requirements in the procedure, it is harder to request financial resources for such investment with no legal basis. This may lead to a situation in which emergency safe rooms are designated in buildings which are not suitable. Moreover, the procedure does not specify the ways of notifying about a threat. In the analysed cases, telephone contact was the method of threat notification. Lack of clearly specified guidelines results in selection of not the best solutions but the cheapest ones which do not require the interference in the infrastructure of the workplace.

Fourthly, the procedure does not specify how to mark emergency safe rooms and alternative emergency safe rooms in such a way that for a bystander or potential attacker they are incomprehensible and at the same time are clearly understandable for employees. Although the employees are familiar with the AT attachment, are trained with regard to the security procedures and participate in drills, in a dangerous situation, stress and panic may lead to irrational behaviours, hence the need for legible demarcation of emergency safe rooms. In the analysed cases, signs depicting semantically neutral objects related to the specificity of the production were used. For a bystander they were meaningless but for the employees who were informed that

these signs signify either the emergency safe room or the gate which will be used for evacuation in case of a terrorist threat.

Sixthly, the first part of the AT attachment – the so-called *Terrorist attack risk assessment table* was designed in such a way that it is exceptionally difficult to obtain a result other that low terrorist risk level for a protected facility, area or equipment. Facilities seem not to be in a direct danger of a terrorist attack - it is questionable if a threat indicator measured using such method is credible.

Seventhly, it is appropriate to include in the AT attachment a procedure to be followed when an unmanned aerial vehicle (drone) appears over a facility. On one hand it may be performing an observation as a part of preparation phase of an attack, on the other hand, it may be carrying explosive materials/CBRN.

Eighthly, in the context of the implementation of the procedures specified in the AT attachment, communication with the employees of a given facility is a very important element. Frequently the personnel is not aware of the existence of a terrorist threat and reacts with condescending smiles when asked to participate in an AT training stressing the pointlessness of such preparations in a *safe country*. Lack of proper security education on the above-school level means that people conducting training related to the AT attachment procedures should not only have necessary general competence for training but above all specialist knowledge of security, anti-terrorism, activity of terrorist organisations and modus operandi of potential attackers to make people aware that the threat is real and following the AT procedures can save their lives.

Ninthly, in the case of the AT attachment, there is no equivalent to *Methodology of acceptance of security plans related to areas, facilities and equipment subject to mandatory protection*. The procedure of AT attachment acceptance is still very general. The information it contains to a large extent depend on the interpretation of the officer who examines the documents in the respective Internal Security Agency local office. Therefore, it would be reasonable to specify the guidelines related to emergency safe rooms, decision-making process in case of an evacuation and standards of evacuation notification. The information on these issues can be obtained through consultations with respective Internal Security Agency local office, however, such procedure prolongs the process of preparation and acceptance of the attachment making it more time consuming for both sides.

Lastly, in the analysed cases, the training related to the AT attachment procedures covers not only the rules of evacuation form a workplace premises but also the general rules on how to behave in a dangerous situation, for example instructions on what to do with a suspicious package, the Run, Hide, Fight rule and developing correct reactions and reflexes: observation of the surroundings and paying attention to suspicious objects or people. The trainings teach also how to behave in a hostage-taking situation and what not to do when anti-terrorist squad enters the premises of a workplace. Therefore, the importance of training in the process of security education and improvement of safety in everyday life is substantial.

ACKNOWLEDGEMENTS

This paper has been financially supported by University of Ostrava, Institutional Development Project (IRP) No. 201819 Social and Cultural Mechanisms of In- and Exclusion: a Comparative Perspective.

REFERENCES

Anti-terrorism. Act from 10 June 2016 (Journal of Laws [Dz. U.], item. 904).

Crisis Management. Act of 26 April 2007 (Journal of Laws [Dz. U.] from 2013 item. 1166 and from 2015 item. 1485.

Ejdys, J., (ed.) 2010. *Kształtowanie kultury bezpieczeństwa i higieny pracy w organizacji.* Oficyna Wydawnicza Politechniki Białostockiej, Białystok.

National Programme for Critical Infrastructure Protection (2018). https://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf

Nogalski, B., 1998. *Kultura organizacyjna. Duch organizacji*. Oficyna Wydawnicza Ośrodka Postępu Organizacyjnego, Bydgoszcz.

People and Property Protection. Act from 22 August 1997 (Journal of Laws [Dz. U.] from 2014, item 1099 and from 2015, item 1505).

Sikorski, Cz., 2012. *Kultura organizacyjna*. C. H. Beck, Warszawa.

Suchacka, M., 2017. *Wybrane aspekty doskonalenia kultury organizacyjnej w kontekście bezpieczeństwa pracy*. Światowy dzień bezpieczeństwa i ochrony zdrowia w pracy, (ed.) Ulewicz, R., Żywiołek, J., Oficyna Wydawnicza Stowarzyszenia Menedżerów Jakości i Produkcji, Częstochowa, 67-84.

https://www.abw.gov.pl/

http://www.policja.pl/pol/kgp/biuro-prewencji/wydzial-nadzoru-nad-sp/specjalistyczne-uzbroj/76255,Liczba-obiektow-podlegajacych-obowiazkowej-ochronie.html

https://rcb.gov.pl/infrastruktura-krytyczna/

https://rcb.gov.pl/zarzadzanie-kryzysowe/