Terrorism – Studies, Analyses, Prevention, 2024, no. 5: 391–409
CC BY-NC-SA 4.0
https://doi.org/10.4467/27204383TER.24.014.19402

Varia

Building resilience of critical infrastructure in the light of asymmetric threats and terrorism

Legislative trends in the Polish implementation of the CER Directive with particular reference to aspects of standardisation and certification of organisational and technical solutions

Adam Tatarowski

The Technical Property Protection Development Institute TECHOM
https://orcid.org/0009-0007-5503-6819

Sources and context of contemporary asymmetric threats and terrorism

In the 1930s. the Soviet Union, through the concepts of Georgii Isserson and Vladimir Triandafillov, set world standards in military thought. Isserson was the first to develop an innovative military doctrine based on the use of deep operations, i.e. striking at the full depth of the enemy's troops, across the entire front line[1]. In the post-Stalin era, colonel Yevgeny Messner developed the concept of warfare by non-military means (so-called 'rebel wars')[2], describing the role of terror in the conduct of military operations, the use of civilians and specific social groups in the fighting, the creation

[1] Г.С. Иссерсон, *Эволюция оперативного искусства*, Москва 1937 (G.S. Isserson, *Evolyutsiya operativnogo iskusstva*, Moskva 1937).

[2] Е.Э. Месснер, *Хочешь Мира, Победи Мятежевойну!, Творческое наследие Е.Э. Месснера*, Москва 2005, (Ye.E. Messner, *Khochesh' Mira, Pobedi Myatezhevoynu!, Tvorcheskoye naslediye Ye.E. Messnera*, Moskva 2005), p. 110.

of paramilitary units in a situation where the differences between a state of war and a state of peace were reduced. These approaches are continuing by General Valery Gerasimov, Chief of General Staff of the Armed Forces of the Russian Federation. In 2013, in a paper widely reported in the media[3], he outlined the assumptions of hybrid warfare, which were based on the synchronised use of military and non-military means by which it will be possible to achieve strategic and political objectives. Gerasimov discussed actions such as the introduction of a contingent of international peacekeepers under the pretext of defending human rights, political isolation, economic sanctions, blockades of land, sea and air communication routes, and threats to use force.

Since 2014, since the invasion of the so-called green men and the annexation of Crimea, all this can be observed in practice - war has been going on basically all the time and is not a continuation of politics, as Carl von Clausevitz wrote about, but an element of it[4]. The Russian aggression, which took full-scale form in February 2022, emphatically demonstrates that the evolution of asymmetric threats has greatly accelerated and is affecting not only the strictly military area, but also the entire security environment. Thus, the concept of asymmetric threats, succinctly described in *the NATO Glossary of Terms and Definitions* as those that result from the ability to use various means and methods to circumvent or neutralise an adversary's strengths and exploit its weaknesses to achieve disproportionate objectives[5], should now be understood much more broadly - in civilisational, social, cultural and technological terms. Moreover, terrorism, the essence of which has always been to deliberately and consciously attack innocent bystanders or social groups with the intention of intimidating state authorities or society, has taken on a much fuzzier form. Collin Powell has rightly observed that while the civilised world has sought for hundreds of years to reduce the destructiveness of wars - through, for example, the civilian-soldier distinction - modern terrorism is increasingly blurring that distinction[6]. The totality of these threats is today becoming

[3] В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер" 2013, (B. Gerasimov, *Tsennost' nauki v predvidenii*, „Voyenno-promyshlennyy kur'yer" 2013), no. 8, pp. 2–3.

[4] C. von Clausewitz, *On war*, Princeton University Press 1976.

[5] *AAP-6 the NATO Glossary of Terms and Definitions,* 2021.

[6] From: J.M. Fish, S.J. McCraw, Ch.J. Reddish, *Fighting in the gray zone: A strategy to close the preemption gap*, Strategic Studies Institute 2004, p. 6.

a challenge for those responsible for protecting critical infrastructure (hereafter: CI) and ensuring its resilience. This article describes legislative trends in this area, with a particular focus on the standardisation and certification aspects of organisational and technical solutions arising from the CER Directive.

Emerging risks in the context of asymmetric threats and contemporary terrorism – challenges in the legal and normative area

The COVID-19 pandemic has significantly accelerated the work started in 2018 on the new technical specification *ISO/TS 31050:2023 Risk management - Guidelines for managing an emerging risk to enhance resilience*, describing approaches to assessing and managing emerging risks that are difficult to predict and understand due to a lack of sufficient data and verified information. Their occurrence, from the perspective of an organisation, e.g. a critical entity[7], can result from unexpected changes in the organisational domain, from technological or social developments, globalisation processes, political turmoil and, more broadly, from the rise of asymmetric threats and terrorism. These risks are characterised by a high degree of uncertainty and can lead to serious consequences in terms of resilience, security and continuity (in operational and business dimensions) of the organisation. Managing them requires continuous monitoring and information gathering as well as flexibility in decision-making.

The current concept of risk assessment in CI is based on the assumptions of the 'core' standard *PN-ISO 31000:2018-08 Risk management - guidelines* and is set in a complex legal and normative environment, in which an 'object-oriented' approach to the emergence of CI entities continues to function. According to the National Critical Infrastructure Protection Programme (NCIPP)[8], this emergence takes place in three stages. The first establishes to which system (according to the NCIPP - e.g. communications,

[7] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Official Journal of the UE L 333/164 of 27 XII 2022).

[8] The National Critical Infrastructure Protection Programme 2023, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [accessed: 29 XI 2023].

health care, ICT networks) the potential CI facility (also: facility, installation or service) belongs and compares its characteristics with the criteria of the respective system (these criteria are classified), the second verifies whether the facility plays the role referred to in the statutory definition[9], and then analyses whether the possible consequences of the destruction or discontinuation of the potential CI will meet at least two cross-cutting criteria relating to the social impact of the destruction or discontinuation of the facility, equipment, installation or service. These criteria include:

- casualties,
- financial implications,
- need to evacuate,
- loss of service,
- recovery time,
- international effect,
- uniqueness (in the sense of the impossibility of replacing and reconstructing the damaged facility, equipment or installation).

Although the 'object-oriented' approach is paralleled by a 'service-oriented' system of selecting operators of essential services within the meaning of the Act on the National Cyber Security System[10], the scope of this regulation is limited, as it applies only to the services included in this Act and only to those relating to information systems. A decision recognising an entity as essential service operator is issued if:

- entity provides essential service,
- the provision of this service depends on information systems,
- incident would have a significant effect resulting in disruption to the provision of essential service by that operator.

This duality, due to the requirements of the Critical Entities Resilience Directive (CER Directive), will soon disappear. In October 2024, national legislation implementing this directive, introducing a 'service' model for the designation of CI entities, is expected to be enacted. The CER Directive introduces a mechanism for state interventionism. In accordance with its provisions, EU Member States become co-responsible for maintaining the availability of essential service and will have the possibility to directly subsidise business entities providing such services. Member states will

[9] The Act of 26 April 2007 on Crisis Management (Journal of Laws 2023, item 122).

[10] The Act of 5 July 2018 on the National Cybersecurity System (Journal of Laws 2023, item 913, as amended).

designate essential services, identify operators and enforce the level of service availability. This is a definite change of approach not only in the citizen-state relationship, but also in the business-state relationship. There are therefore major challenges ahead for CI. The critical entity will be required to carry out its own risk assessment, based on *PN-ISO 31000:2018-08 Risk management - guidelines*, but taking into account the broadest possible spectrum of risk factors, including those that are considered *emerging risks.*

Risk assessment in critical infrastructure – new approaches

CI operators use different safety management methodologies, depending on their awareness, level of knowledge and understanding of the area they are dealing with. Each recognised methodology is based on a template, which is the standard *PN-ISO 31000:2018-08 Risk management - guidelines*. This standard involves the implementation of the risk management process in three steps:

1) establishing the context,
2) risk assessment (threat identification, risk analysis and estimation),
3) a decision to deal with the risk.

Most of the security management methodologies used in Poland and in countries that are recognised as leaders in this area (e.g. Germany, Sweden, Canada, USA, Ireland, the Netherlands or Australia) are based on this standard. The authors of the publication *Managing Critical Infrastructure Security and the Continuity of Essential State Services*[11] extensively analyse the approaches to risk assessment and management used in these countries and present the Situational Management of Safety Critical Infrastructure (SMSCI) methodology together with the Integral Model for the Security of Critical Infrastructure (IMSCI), which in turn is the tool base of the SMSCI methodology. The stages of this management are:

– establishment of a team,
– definition of safety thresholds,
– mapping of CI characteristics,
– generation of adverse event scenarios,

[11] M. Kisilowski et al., *Zarządzanie bezpieczeństwem infrastruktury krytycznej i ciągłością usług kluczowych państwa* (Eng. Managing Critical Infrastructure Security and the Continuity of Essential State Service), Warszawa 2021.

– formulation of the decision problem,
– risk estimation,
– implementation of safeguards.

In an era of increasing asymmetric threats, including those related to terrorist activities, a valuable supplement (and, above all, help and support) when carrying out risk assessment – within the framework of e.g. the SMSCI methodology – by critical entities are standards or technical specifications, such as:

– *PN-EN IEC 31010:2020-01 Risk management – Risk assessment techniques*,
– *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience*,
– *ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management*.

The critical entity's ability to anticipate, prepare for and respond to different circumstances should be the most important requirement for effective risk management. The critical entity should[12], among other things:

– optimise communication inside and outside the organisation,
– establish an effective way of gathering up-to-date information on emerging risks,
– counteract disinformation,
– develop a way for those responsible for risk management to influence management,
– build trust within the organisation and with collaborators, including government,
– encourage and empower relevant people in the organisation to report what they consider to be significant signals related to the potential occurrence of new risks.

The risk identification process requires the critical entity to be aware of the dynamic changes taking place in the environment in which it operates. Despite the implementation of a risk identification structure (based on the above-mentioned standards or other documents, e.g. relating to terrorist threats[13]), it should also use non-standardised, unstructured

[12] *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience*.

[13] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on the combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (Official Journal of the UE L 88/6 of 31 III 2017).

identification methods, as this will provide a more complementary approach to the problem and increase the effectiveness of identification. According to the *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience*, the organisation should, among other things:

- regularly, comprehensively and from multiple perspectives analyse the environment in which it operates, or use appropriate methods or techniques to identify emerging changes that may give rise to *emerging risks*,
- analyse trends and circumstances that may lead to *emerging risks*,
- analyse sources of risk and possible scenarios of events,
- update descriptions of possible risks on a continuous basis.

Examples of changing circumstances that can be sources of *emerging risks*:

- natural hazards, e.g. climate, weather,
- risks from new bacteria, viruses, fungi and parasites, or from these micro-organisms becoming resistant to available drugs,
- challenges related to the uncontrolled development of the internet of things (IoT),
- challenges related to the development of artificial intelligence.

The latter are an increasingly topical problem and, in the opinion of the author of this article, will soon become a major generator of *emerging risks*. For the first time in human history, devices and systems are being designed whose operation is not fully understood. It is not clear, for example, how Chat GPT works. The developers of this tool understand machine learning algorithms, but how neural networks work (and they have a very fast pace of development) has not been understood exactly. It is also unclear to what extent artificial intelligence will become autonomous, and the delegation of decision-making capabilities to machines, the lack of transparency and understanding of the functioning of artificial intelligence as well as the lack of human oversight may result in previously unknown risks.

Emerging risks may also involve terrorist threats in a broad sense - not just those implied by the definitions in *the NATO Glossary of Terms and Definitions* and the European Parliament's 2017 Counter-Terrorism Directive cited earlier. It must be assumed that the new reality modelled by *emerging risks* will have an impact on the way terrorist crimes are prepared and executed.

In general, the results of a systematic risk assessment by critical entities should include:

- a list of suppliers (resources, services) critical to the critical entity,
- a list of processes whose disruption may cause a critical incident,
- a list of CI necessary to maintain the essential service.

The risk assessment will be the starting point for developing and implementing adequate organisational and technical solutions.

Standardisation and certification of adequate organisational and technical solutions under the CER Directive

Outline of the CI protection regime in the light of the NCIPP 2023 and the CER Directive

Within the framework of the NCIPP, there is a so-called six-pack describing the CI security system. The measures taken to ensure the security of CI include:

1) ensuring physical security - a set of organisational and technical actions aimed at minimising the risk of disrupting CI operations as a result of actions of persons who have attempted to enter or have entered CI in an unauthorised manner;
2) ensuring technical security - a set of organisational and technical measures aimed at minimising the risk of disrupting the functioning of CI as a consequence of disrupting the technological processes in progress;
3) ensuring personal security - a set of organisational and technical activities aiming at minimising the risk of disrupting CI operations as a result of actions of persons who have authorised access to critical infrastructure;
4) ensuring ICT security - a set of organisational and technical measures aimed at minimising the risk of disrupting CI operations as a result of unauthorised interference with control apparatus and ICT systems and networks;
5) legal assurance - a set of organisational and technical measures aimed at minimising the risk of disrupting CI operations as a result of legal actions of external entities;

6) business continuity and restoration plans, understood as a set of organisational and technical actions leading to the maintenance and restoration of the functions performed by CI[14].

This system corresponds to Article 13 of the CER Directive *Resilience measures of critical entities*. The first paragraph of this article reads:

1. Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:
   a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;
   b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access control;
   c) respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;
   d) recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;
   e) ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;
   f) raise awareness about the measures referred to in points a) to e) among relevant personnel, duly considering training courses, information materials and exercises.

   For the purposes of the first subparagraph, point e), Member States shall ensure that critical entities take into account the personnel of external service providers when setting out categories of personnel who exercise critical functions.

[14] The National Critical Infrastructure Protection Programme 2023...

The CER Directive, which is the standard in European legislation, allows Member States to regulate on a case-by-case basis the provisions of national law implementing its provisions in such a way that the level of resilience of critical entities is as high as possible and compatible with national specificities, but taking into account the use of standards, as referred to in Article 16 of the Directive.

A standard is a normative document adopted by a recognised standardisation body. In Poland this is the Polish Committee for Standardisation. A standard establishes principles, guidelines or characteristics for different activities and their results, is approved by consensus, is intended for widespread and repeated use, is accepted by all interested parties as a benefit to all, and introduces a code of good practice and principles of rational conduct at the current level of technology[15].

The use of standards in the standardisation and subsequent certification of organisational and technical solutions is the right step in building the resilience of CI to all types of threats. It facilitates the selection of solutions, their maintenance and validation, and allows for effective oversight and enforcement, as the national authority overseeing CI - in accordance with Article 21 of the CER Directive - will inspect and make decisions based on data collected by external competent auditing and certification entities.

The range of organisational and technical solutions that should be applied to a critical entity following a risk assessment is very broad. In order to present synthetically the issue of standardisation and certification, the author of the article referred to technical measures to ensure physical security, which are a good point of reference for this topic, as well as to ensure business continuity of essential services.

Standardisation and auditing - the context of standardisation

According to the concept presented by the author of this article on 5 October 2023 at *the National Forum for Critical Infrastructure Protection*[16], organisational and technical solutions implemented by critical entities should be created in accordance with standards, which makes it possible -

[15] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation (Official Journal of the UE L 316/12 of 14 XI 2012).

[16] A. Tatarowski, *Standardisation and Certification of CER Directive Solutions, 10th National Forum for Critical Infrastructure Protection*, Warszawa 2023, https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami.

due to the availability of legal and business solutions - to conduct audits and certifications effectively. An audit is (...) *a systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which audit criteria are met*[17]. An audit assesses compliance now and in the past, may have a legal and normative purpose and should meet business needs. It is based on seven principles:

1) reliability as a basis for professionalism,
2) honesty in the presentation of results,
3) professional due diligence,
4) confidentiality,
5) independence,
6) an evidence-based approach,
7) a risk-based approach.

There are three types of audits (Table 1).

Table 1. Types of audit according to the standard PN-EN ISO 19011:2018.

1ST party audit	2ND party audit	3RD party audit
Internal audit	External provide audit	Certification and/ or accreditation audit
	Other external interested party audit	Statutory, regulatory and similar audit

Source: *PN-EN ISO 19011:2018 Guidelines for auditing management systems.*

From the perspective of critical entities, the most relevant is the third-party audit, which is carried out by independent auditing organisations, such as certification bodies or government institutions. The government institution overseeing critical entities in Poland (in the legal conditions that will follow the implementation of the CER Directive) will collect data and make decisions on the basis of (...) *evidence of the effective implementation of these measures* [i.e. Article 13 measures, discussed as organisational and technical solutions], *including the results of an audit conducted at the entity's expense by an independent and qualified auditor selected by the entity.* Evidence in a third-party audit is to be understood as certificates, i.e. documents issued by a conformity assessment body (certification body), confirming

[17] *PN-EN ISO 19011:2018 Guidelines for auditing management systems.*

that a product/installation/system/process/service complies with the requirements. In the case of the implementation of the CER Directive, compliant with the requirements contained in the relevant standards.

As an aside, it is worth clarifying one of the aspects that the author of this article encounters in his professional activity as the head of a certification body. Conformity assessment always refers to a document, in this case a standard. Referring to standards in legal regulations, even though they are documents for so-called voluntary application, is possible, which is confirmed by the position of the President of the Polish Committee for Standardisation[18] and by court judgements[19]. Thus, if a standard is referred to in the provisions of a law, then referring to it (e.g. in the case of an audit or certification) is possible and justified. Such practice is present in Polish legislation, e.g. in the Act on the National Cybersecurity System. However, the citation of standards in the legislation does not facilitate insight into them. Access to these standards is chargeable.

Conformity assessment. Competence of certification bodies and auditors to carry out certification. Certificate versus declaration of conformity

A third party audit may be conducted by a conformity assessment body (certification body) accredited under the provisions of the Act on Conformity Assessment and Market Surveillance Systems[20] - and such a solution already exists with regard to security auditing of an information system used to provide essential service[21] - or by a certification body authorised to certify on behalf and for the benefit of the Polish Committee for Standardisation within the meaning of the provisions of the Act on Standardisation[22]. Certification should be understood as the action of a conformity assessment body (certification body) demonstrating that a product/installation/system/process/service complies with

[18] *Voluntary application of standards*, the Polish Committee for Standardisation, https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn [accessed: 29 XI 2023].

[19] Judgement of the Supreme Court of 10 April 2019, II OSK 1486/17; Judgement of the Voivode ship Administrative Court in Kielce of 19 May 2009, II SA/Ke 183/09.

[20] The Act of 13 April 2016 on Conformity Assessment Systems and Market Surveillance (Journal of Laws of 2022, item 1854).

[21] The Act on the National Cybersecurity System ("ANCS") – (Journal of Laws 2023, item 913, as amended).

[22] The Standarisation Act of 12 September 2002 (Journal of Laws of 2015, item 1483).

the requirements. The empowerment of certification bodies is very strong. They function as components of an overall European system encompassing conformity assessment and market surveillance[23] and their use in auditing and certifying organisational and technical solutions implemented by critical entities will become essential.

It is worth noting that the term 'certificate' is often used in an unauthorised way (from the perspective of the conformity assessment system). According to a dictionary definition, a certificate is 'an official document stating, for example, the conformity of a product with standards, the authenticity of a work of art or the completion of a course'[24]. The Council for the Polish Language at the Presidium of the Polish Academy of Sciences has also taken a position on the concept of a certificate[25]. In the context of the conformity assessment system - the conformity that will be decisive in the case of CI - a certificate is therefore, as already mentioned, a document issued by a conformity assessment body (certification body), confirming that a product/installation/system/process/service complies with the requirements.

This is an authorial definition, as this concept in relation to conformity assessment with non-harmonised standards has never been defined. There is no such definition in the provisions on standardisation - both in the Act in question and in the Regulation of the Council of Ministers on the method of granting and using the mark of conformity with the Polish Standard[26], which even indicates the template of the certificate. Moreover, there is no definition of a certificate (in the terms indicated by the author of the article) in the Act on Conformity Assessment and Market Surveillance Systems. It only defines a certificate as an attestation of conformity issued by a notified body, i.e. one that has been notified to the European Commission and is on the list of bodies notified for specific directives and therefore

[23] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Official Journal of the UE L 218/30 of 13 VIII 2008).

[24] *Polish Language Dictionary PWN,* https://sjp.pwn.pl/sjp/certyfikat;2553201.html [accessed: 29 XI 2023].

[25] *Position of The Council on the use of the word certificate,* https://rjp.pan.pl/dokumenty-rady?view=article&id=98:stanowisko-rady-wobec-uycia-sowa-certyfikat&catid=45 [accessed: 29 XI 2023].

[26] Regulation of the Council of Ministers on the method of granting and using the mark of conformity with the Polish Standard (Journal of Laws of 2010, no. 198, item 1316).

carrying out a mandatory conformity assessment. Given the needs arising from the CER Directive, a clarification of the concept of certificate in national legislation is expected.

The declaration of conformity is defined in the Act on Conformity Assessment and Market Surveillance Systems. This declaration is to be understood as a statement by the manufacturer, installer or their authorised representative or private importer (under their sole responsibility) that the product complies with the requirements.

What attitude to the importance of such a declaration could be observed in practice? A good, model example of an industry in which, for years, there has been a small but powerful lobby promoting the idea that a declaration of conformity is sufficient and guarantees compliance with requirements and quality is the industry of technical physical security measures. Nowadays, such voices have almost disappeared - due to a completely different awareness of market participants and government representatives, which has been altered by negative experiences. Below are some examples illustrating how the market has operated - and in some areas still operates. On 7 September 2010, the ordinance was published by the Minister of Internal Affairs and Administration on the requirements to be met for the protection of monetary values stored and transported by entrepreneurs and other organisational units[27]. In § 12 of this regulation, there is a point stating that for the storage or transport of monetary values, equipment shall be used (...) *with a certificate of conformity issued by an authorised certification body or a declaration of conformity issued by the manufacturer or importer, attesting compliance with the essential or specific requirements within the meaning of the provisions on the conformity assessment system, where such requirements have been established for the product.* These provisions are still valid. Intuitively, it is known that if an equipment supplier has the opportunity to market a device that has a declaration of conformity that he himself issues, which most often has no factual basis, he will not carry out tests in an accredited laboratory and seek certification. The investor has no scope for action in this case. A more recent example is the 2012 Waste Act[28]. The waste holder is obliged to maintain a visual control system for the storage or disposal site. The implementing act of this

[27] Ordinance of the Minister of the Interior and Administration of 7 September 2010 on the requirements to be met for the protection of monetary values stored and transported by entrepreneurs and other organisational units (Journal of Laws of 2016, item 793).

[28] The Waste Act of 14 December 2012 (Journal of Laws of 2023, item 1587, as amended).

law[29] specifies that: *The parameters of the technical equipment of the control system shall meet at least the requirements of the PN-EN 62676-4: 2015-06 Video surveillance systems for use in security applications - Part 4: Guidelines for use or a standard to replace the standard in question*. Unfortunately, most waste holders (perhaps even none) do not have such a system in place. Why is this the case? Leaving aside the less than ideal wording of this provision, it lacks any indication of how to confirm compliance that an installed CCTV system meets the requirements. The designer therefore bears no risk if he designs such a system without even knowing the referenced standard (the phenomenon of low levels of competence is common in the industry, but there are legal and normative solutions that are already beginning to work, as will be described later in this article), nor does the installer who installs such a system and issues a declaration of its compliance with the standard. Such systems, if they work at all, often fail to meet the needs of the investor and the requirements of the standards, and are, of course, unreliable. This is how a large area of the market operates.

In the case of CI, which - according to the CER Directive - must develop resistance to asymmetric threats, terrorist acts and other threats, such an approach is unacceptable. The technical security system (intrusion detection system, video surveillance system, access control system) should be certified after installation. Services provided by external entities (i.e. design, installation, maintenance) to CI should meet the highest quality standards. These entities should be certified to the standard *PN-EN 16763:2017 Services for fire safety and security systems,* which fulfils the requirements of Article 13(1)(e) of the CER Directive. This directive addresses the need to sort out the requirements for service providers (including in the area of fire protection), as the author of this article has repeatedly stated at various industry events and conferences[30].

[29] Ordinance of the Minister of the Environment on a visual inspection system for the place of waste storage or disposal (Journal of Laws of 2019, item 1755).

[30] A. Tatarowski, *Nowe sposoby walidacji jakości usług projektantów, instalatorów i konserwatorów systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych w procesie budowlanym*, IV Międzynarodowa Konferencja N-T "Problemy Inżynierii Bezpieczeństwa Obiektów Antropogenicznych" (Eng. New ways to validate the quality of services of designers, installers and maintainers of fire protection and technical security systems in the construction process, 4th International Conference "Problems of Safety Engineering of Anthropogenic Facilities"), Warszawa 2021, https://psribs.pl/conferences/iv-miedzynarodowa-konferencja-n-t-problemy-inzynierii-bezpieczenstwa-obiektow-antropogenicznych-wiosna-2021/ [accessed: 29 XI 2023]; A. Tatarowski, *Nowe*

The aforementioned standard has already been cited as relevant for assessing the competence and qualification of operators in this industry in Annex 1 *Standards for ensuring the efficient functioning of critical infrastructure - good practices and recommendations* to the NCIPP 2023.

Implementation, maintenance and certification of essential service business continuity management system

A critical entity that has carried out a risk assessment and is implementing (or has implemented) adequate organisational and technical measures should implement essential service continuity management system in accordance with the standard *PN-EN ISO 22301:2019 Security and resilience. Business continuity management systems. Requirements.* A business continuity management system based on the aforementioned standard consists of the following elements:

a) a policy,
b) competent people with defined responsibilities,
c) management processes relating to:
    1) policy,
    2) planning,
    3) implementation and operation,
    4) performance assessment,
    5) management review,
    6) continual improvement,
d) documented information supporting operational control and enabling performance evaluation.

Essential services are usually not provided by a single operator - it is most often a collection of several services that operate independently of each other and are provided by different operators. A good example of essential service - as the authors of the publication *Managing Critical Infrastructure Security and Continuity of State Essential Services* point out - is withdrawing money from an ATM. In order to be able to withdraw cash, the component services must be available in the form of:

sposoby walidacji jakości usług projektantów, instalatorów i konserwatorów systemów ochrony przeciwpożarowej, XXIX Ogólnopolskie Warsztaty – Sygnalizacja i Automatyka Pożarowa SAP '2023, Żnin 2023 (Eng. New ways to validate the service quality of designers, installers and maintainers of fire protection systems, 29th All-Poland Workshop - Fire Signalling and Automation SAP '2023, Żnin 2023), https://www.polon-alfa.pl/pl/aktualnosci/polon-alfa-w-cukrowni-%C5%BCnin [accessed: 29 XI 2023].

1) availability of power supply to the ATM,
2) availability of the Internet network providing connectivity to the billing system,
3) availability of the billing system of the bank from which the money is withdrawn,
4) the provision of cash at the ATM, which is currently mainly the responsibility of ATM network operators.

Thus (...) *the possibility of withdrawing money from an ATM is in fact a set of relations that exist between the said component services and can only occur as a result of the simultaneous availability of all component services. Consequently, the unavailability of one of the component services of essential service is sufficient for it also to be unavailable*[31].

Given the complexity of essential services, the use of IM-SCI supplemented by standards may be helpful. Several ways to ensure uninterrupted access to the service have been described in the literature. These include:

– structural redundancy, which involves the duplication of elements deemed critical,
– functional redundancy, which consists in adapting selected elements of the system to perform additional functions,
– parametric redundancy, which consists in standardising the system to a degree that exceeds ensuring its usefulness[32].

It is worth noting the way called functional redundancy. Using IM-SCI:

> (...) a governmental institution, e.g. the Government Centre for Security, can, using the list of essential services, identify the entities that provide the constituent services for the essential services. The constituent services can then be treated as functionalities of the CI facilities under consideration. In the event of an incident limiting

[31] M. Kisilowski et al., *Zarządzanie bezpieczeństwem infrastruktury krytycznej...*, p. 106.

[32] K. Szwarc, *Modelowanie ciągłości działania systemów zarządzania kryzysowego i ocena przydatności rozwiązań na szczeblu lokalnym*, rozprawa doktorska (Eng. Modelling business continuity of crisis management systems and assessing the usability of solutions at local level, PhD thesis), Warszawa 2019, https://repo.bg.wat.edu.pl/info/phd/WATefc9a9340f3e47cb8141566cdf6e0e53/Record+details+%25E2%2580%2593+Modeling+of+the+continuity+of+crisis+management+systems+and+the+assessment+of+suitability+at+the+local+level+%25E2%2580%2593+Military+Technical+Academy+them.+Jaroslaw+Dabrowski+title?aq=%40status%3Apracownik%2Cauthorprofile%2F%40possitionPL%21%3Aadiunkt%2Cauthorprofile%2F%40possitionPL%21%3Aprofesor%2C%40active%3D%27true%27%2C.%3AWUT84b1c97cce2d442fab1acdc256a5d487&r=author&ps=20&lang=en&pn=1&cid=157628.

> or eliminating the availability of CI functionality, it is possible to identify CI facilities with similar functionality and, as part of the BCP (i.e. Business Continuity Plan), complement the missing component essential service with functionality provided by another CI facility[33].

The issue of developing, implementing and certifying a business continuity management system is vast and unique to each critical entity. The quoted excerpts taken from the literature are intended - by the author of this article - to encourage readers to expand their knowledge in this area, as this issue is the most relevant part in the overall view of the CI security management system.

In summary, from the perspective of the critical entity, an important activity will be the continuous improvement of the business continuity system through the use of effectiveness measurement, including simulation, monitoring, systematic review, incident assessment and effective removal in accordance with the security policy. One of the measurement tools will be to conduct systematic and independent audits, including those culminating in certification, but to the extent necessary to maintain the provision of the essential service.

Summary

The year 2024 will be a breakthrough year for CI. The pressing deadlines, obliging member states to enact national legislation implementing the CER Directive, require the preparation of an appropriate environment for effective legislative work. The Government Centre for Security, which for many years has been creating conditions conducive to improving the security of CI and has built an approach to security management in the sector that is unique in the EU, based on the aforementioned so-called 'six-pack', is now facing a major challenge in developing the implementation of the CER Directive in Poland. This article presents the legislative trends related to this implementation in terms of standardisation and certification of organisational and technical solutions. Standardisation and certification of these solutions based on standards will allow for the replacement of direct control by government, enable faster, more effective and optimal

[33] M. Kisilowski et al., *Zarządzanie bezpieczeństwem…*, p. 108.

adaptation of the resilience of critical entities to asymmetric, terrorist and those arising from or involving emerging risks.

In 2024, hybrid activities originating in the East, but also in other regions of the world, are expected to intensify. This makes the need for legislative regularisation not only in relation to CI, but also in the broader legal area, including: *the Act of 22 August 1997 on the Protection of Persons and Property, the Act of 26 April 2007 on Crisis Management, the Act of 10 June 2016 on Anti-Terrorist Activities and the Act of 11 March 2022 on the Defence of the Homeland.*

Adam Tatarowski

Director of the Technical Property Protection Development Institute TECHOM - a specialised certification body and a continuing education institution. It trains, among others, functionaries involved in the protection of persons and objects in the uniformed services, CI employees responsible for security and service providers carrying out projects, installations and maintenance of fire protection systems and technical means of ensuring physical security. The author is a specialist in assessment of compliance of technical means ensuring physical security (and services in this area), an expert of Technical Committees no. 52, 264, 306 and 323 of the Polish Committee for Standardisation.

Contact: tatarowski@techom.com