DOI: 10.53477/1841-5784-21-15

CRITICAL INFRASTRUCTURE PROTECTION POLICY IN THE EU

Miklós BÖRÖCZ*

It represents a possibility that some of the terrorist attacks will be directed against critical infrastructure in the future. An example in this regard is the attack on a water treatment plant in the U.S., where an intruder attempted to raise sodium hydroxide levels more than a hundredfold thus poisoning drinking water supplies. The importance of protection is also illustrated by the cyber-attack on Düsseldorf Hospital in December 2020, when an attack on critical infrastructure has led to a fatal incident in Europe for the first time. At the same time, critical infrastructure protection is further enhanced in the event of a possible hybrid warfare or war situation. Its importance in practice was also illustrated by the Russian-Ukrainian conflict in December 2015, when the BlackEnergy APT group caused a power outage in Ukraine affecting two hundred and twenty-five thousand people. This attack has shown what success an unconventional military element can achieve in the world of current levels of energy use. This study aims at presenting the risks that critical infrastructures involve, followed by the sectors with European critical infrastructures and their main characteristics, as well as some key European infrastructures.

Keywords: *critical infrastructure protection; vulnerability; hybrid warfare; non-linear strategy; threat; cyberattack.*

***** Miklós BÖRÖCZ is a former police lt. colonel, PhD. Candidate in EU security policy within Óbuda University in Budapest, Hungary. The former Chairman of the Hungarian Counter Terrorism Centre (CTC)'s Scientific Council. The former member of the Ministry of the Interior's Scientific Council, Budapest, Hungary. E-mail: boroczbat@gmail.com***

Introduction

In the field of critical infrastructure protection, the United States of America recognized as a pioneer that no state, however powerful, could single-alone protect its own infrastructures, so it initiated international cooperation in this area.[1] US's idea was first taken up by NATO, who encouraged its Member States to take measures in order to protect their critical infrastructure through studies and impact assessments. The European Union then joined the initiative, and its actions will be summarized on the subject hereinafter.

Firstly, I think it is important to examine the international security environment that significantly changed, which is also strongly relevant for critical infrastructures. Important findings in this area have already been formulated in the study National Security and Critical Infrastructure Protection[2]. Today, the concept that nation states and their citizens feel safe whether or not they can win a war with the help of their regular forces has changed. With the emergence of weapons of mass destruction, this approach has been overshadowed, as nuclear weapons, for example, affect the military power of both parties. Thus, the strategic approach gradually loses its importance, replaced by political instruments and economic interventions and sanctions. After The Second World War, welfare societies were established where the continuous availability of water, food, energy, transport and other supplies and services wakens security for countries and their citizens. At the same time, the vulnerability of infrastructures in sectors and thus their protection has been appreciated. Defence is now hampered by the serious spread of proliferation and the challenges posed by asymmetric warfare, which has evolved but is constantly evolving, and which continues to take advantage of technical innovations.

These new types of threats have thus transformed traditional security paradigms, since powerful military forces can no longer guarantee the social peace of states today.

At the same time, there have been changes in the military thinking of Russia, one of the most dangerous to NATO and the European Union.[3] Its essential element is hybrid warfare (which is originally different from the definition of Chechen

[1] Toma Virgil, "Evoluția conceptului de infrastructură critică" [The evolution of the concept of critical infrastructure], in *Inspectoratul pentru Situații de Urgență al Județului Argeș*, URL: http://www.igsu.ro/documente/publicatii/articole_de_specialitate/Evolutia_conceptului_de_infrastructura_critica.pdf, accessed on 27.02.2021.

[2] Adriana Alexandru, Victor Vevera, Ella Magdalena Ciupercă, "National Security and Critical Infrastructure Protection", in *International Conference Knowledge-Based Organization*, vol. XXV, No 1/2019, DOI: 10.2478/kbo-2019-0001, pp. 8-13.

[3] Krisztián Jójárt, "A hibrid hadviselés orosz elméletének változása az ukrajnai tapasztalatok tükrében" [The change of the Russian hybrid warfare's theory in the light of the Ukrainian experiences], in *Hadtudomány*, No. 1-2/2019, pp. 49-60.

warfare formulated by William J. Nemeth), in which Moscow implements irregular and conventional warfare as a state entity, as it does now in Ukraine. In his analysis[4], the Director of the Carnegie Moscow Center further explained that hybrid war is a new era of opposition between Russia and the "West", which can be interpreted, among other things, as an analogy to the Cold War. According to Aleksandr Bartos of the Russian Academy of Military Sciences, "hybrid wars are in fact transformed into a new type of international opposition and, in addition to strategic nuclear deterrence, they are an effective non-nuclear deterrent to Russia's adversaries."[5] In his well-known analysis, he suggests that hybrid war will become the defining form of warfare of the future Bartos explained in another analysis that the "reunification" of Crimea and its participation in the Syrian civil war showed the success of the Russian non-linear strategy.[6] He also explained that hybrid war is aided by a lack of legitimacy and international norms, which allow for covert operations involving terrorists, organized criminals, cybercriminals and private military companies.[7]

In Ukraine, between July 2014 and July 2018, several critical infrastructures (energy supply, transportation, drinking water supply, banking system, and financial markets) were attacked by hacker groups linked to Russia. In July 2014, Russian hacker groups CyberBerkut and GreenDragon entered the PrivatBank system unauthorized and disclosed confidential information (account details, phone numbers, etc.). On the 23rd of December, 2015 the APT 28 group after several months of preparatory work has disturbed the electricity system operators of Kyiv, Prykarpattia, and Chernivtsi with remote access. The attack left about two hundred and twenty-five thousand consumers without energy and heating for six hours. This was the first publicly documented successful cyberattack against an electrical network control system.[8] A malware called BlackEnergy was also discovered in

[4] Dmitri Trenin, "Avoiding U.S.- Russia Military Escalation During the Hybrid War", in *Carnegie Moscow*, URL: https://carnegie.ru/2018/01/25/avoiding-u.s.-russia-military-escalation-during-hybrid-war-pub-75277, accessed on 17.04.2021.

[5] Aleksandr Bartos, "Россия в эпоху гибридных войн" [Russia in the era of hybrid wars], in *He3abncnmoe*, URL: http://nvo.ng.ru/gpolit/2017-10-20/1_970_hybrid.html, accessed on 17.04.2021.

[6] Aleksandr Bartos, "Гибридная война – переход от неудач к победе [Hybrid warfare – Transition from Failure to Victory]", in *He3abncnmoe*, URL: https://nvo.ng.ru/realty/2018-06-01/1_998_hybryd.html, accessed on 17.04.2021.

[7] Aleksandr Bartos, "Гибридная война – новый вызов национальной безопасности России", [Hybrid war is a new challenge to Russia's national security], in *Национальная Оборона*, URL: http://www.nationaldefense.ru/includes/periodics/maintheme/2017/1016/154222573/detail.shtml, accessed on 17.04.2021.

[8] David E. Whitehead, Kevin Owens, Dennis Gammel, Jess Smith, "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies", in *Power and Energy Automation Conference* Spokane, Washington, March 21–23, 2017, URL: https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf, accessed on 20.04.2021.

time, a month later at the network of Borispil International Airport, near Kiev, so their attack was unsuccessful. Researchers say previous attacks can be paralleled by smaller attempts made between November and December 2015, targeting Ukrainian mining and rail systems (with malware such as KillDisk and BlackEnergy). In 2017, the NotPetya extortion virus (which originally targeted Ukraine but affected business circles worldwide) affected several critical infrastructure sectors. The cyberattacks targeted the Ukrainian government, the energy sector (the Chernobyl Radiation Monitoring Station), the banking sector (the National Bank of Ukraine and ATMs nationwide), and the transport sector (the electronic payment system for the metro in Kiev). In July 2018, the Ukrainian Security Service managed to crack down on a sabotage operation against a Ukrainian drinking water supply. Due to the prominent role of infrastructure, if the attack had been successful, it would have caused serious water supply problems at national level.[9]

In summary, critical infrastructures are at the crossroads of attacks, not only in the future, but also in the present. The reason for this is that, on the one hand, the increase in living standards in welfare states has transformed people's sense of security, leading to a steady fading of current military doctrines. The states of the West (from which it deviates due to the US forces) now rely more on their political, intelligence and economic power to guarantee social security in their national strategy, which is also evident at the international level (e.g. Smart defence). On the other hand, NATO, and Russia, which currently poses the greatest threat to its member states, have also undergone a paradigm shift in their military strategy. Hybrid warfare, which has been tested and practiced, has brought success to Moscow not only in Syria, but also in Ukraine. Although Russia accuses the West of waging war on it, it was he who perfected the latest form of warfare, which can also be interpreted as an analogy to the "Cold War," so one should expect its protracted time. The main tools for these are cyber-attacks, which are explained in the next chapter. Its targets are critical infrastructures that, if successfully attacked, could cause disruptions in societies that could be prerequisites for a successful regular military operation. Fortunately, this risk has been recognized by the European Union and its Member States in good time and important steps have been taken to reduce these risks. The next section presents the sectors concerned and their main characteristics.

[9] Andreas Marazis, Rober Kothe, "Russian Cyberwarfare Capabilities: Assessing the Threat for Ukrainė s Critical Infrastructure", in *European Neighbourhood Council Analysis*, 2018, URL: http://www.encouncil.org/wp-content/uploads/2018/09/Russian-Cyberwarfare-Capabilities-Assessing-the-Threat-for-Ukraines-Critical-Infrastructure.pdf, pp. 4-6, accessed on 20.04.2021.

1. Sectors and Main Features of Critical Infrastructures

A sectoral and subsector list of European critical infrastructures is defined in Annex I of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

This means that the energy sector is split into subsectors that are electricity (infrastructures and installations for electricity generation and transmission in terms of electricity supply), oil (oil production, refining, processing, storage and fixed transport) and gas (gas production, refining, processing, storage and fixed transport).

The transport sector is divided into subsectors, meaning road (motorways, motorways, bridges, vehicles carrying dangerous substances, public transport vehicles, etc.), railway (railway tracks, railway stations, railway crossing points, railway trains, etc.), air (aircraft, air traffic control systems, airports, heliports, etc.), inland waterways, oceanic and short sea shipping and ports (coastlines, ports, ships, river sections, etc.). The sector can be used to move people and goods quickly and safely.

I also consider important to define the main characteristics of critical infrastructures. Thus, the first characteristic is interdependence, which shows how strong are the links between systems, meaning that one sector (and this is true for subsectors) is not operational without the other sector. Among them: "Some sectors of critical infrastructure depend mainly on the electricity and telecommunications systems and cyber risks. It can be said without exaggeration that the consequences of electricity outages affect all sectors". Critical infrastructure interdependency can be grouped physically, information technologically (cyberly), geographically, and logically.[10] Physical dependence arises where the normal functioning of the sector requires another sector. IT dependency is when the sector is managed by information technology. Geographical dependence is when sectoral elements are installed in geographical proximity to each other and thus interact in the event of a malfunction. Logical dependence is primarily found in relation to the human factor.[11]

The following characteristic is the networking, which means interconnected critical infrastructures, a complex system whose sectoral elements interact continuously with each other.

[10] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies", in *IEEE Control Systems Magazine*, vol. 21, No. 6, 2001, pp. 11-25.

[11] Attila Horváth, "A létfontosságú rendszerelemek és a technológiai fejlődés új kockázatai II. rész, [New Risks of Critical Infrastructure and Technological Development. Part II.]", in *Hadtudomány,* 2016, pp. 216-228 (electronic page number), URL: http://mhtt.eu/hadtudomany/2016/2016_elektronikus/horvathattila22.pdf, accessed on 05.05.2021.

Interdependence and networking can be inferred directly from the domino principle, or domino effect, as a feature of critical infrastructures. This means that damage to a critical infrastructure sector can have an impact on the functioning of several sectors, which together can have a serious social, economic and thus political impact. One of the main examples of this was the power outages in Italy and Switzerland in 2003, which quickly reached Austria, Slovenia and France. Between 50 million and 60 million people were left with no electricity as a result of the event.

Each critical infrastructure sector is characterised by an operational specificity that can be applied individually to that sector.

Expansion and location are very important features of critical infrastructures. A poor placement may lead to disaster, as demonstrated by the installation of safety diesel generators to cool Fukushima reactors in non-flood-free areas, which has significantly helped to cause the disaster. We can also take the location of CERN, whose LHC accelerator (Large Hadron Collider) is very close to Geneva Airport, as an example.

IT, as the main feature of critical infrastructures, shows that all sectors operate almost fully automated using IT systems. Therefore, all necessary protective measures should be taken to ensure that no sector is successfully attacked in the territory of a Member State, as defined in the introduction.

In the following phase, I will present the key infrastructures for the EU based on sectors and key characteristics.

2. Priority European Critical Infrastructures

The list presents, in order of importance, a personal opinion, where it is important to note that the specification is not exhaustive, but merely as an example.[12] Infrastructures for high-voltage electricity networks (e.g. the totality of the networks of the UCPTE Member States referred to above, or the planned Baltic Ring and the Mediterranean electricity ring) and the interconnected sectors and subsectors, such as system controllers or other priority transformer stations.

The Pan-European gas supply network and its facilities can also be regarded as a European critical infrastructure of paramount importance, with its storage, transport and use elements vital for other sectors, as well as for EU Member States and EU citizens.

[12] Tünde Bonnyai, *A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében, [Analysis of the critical infrastructure protection in the light of population training]*, in Ph.D. Dissertation, National University of Public Administration, Doctoral School of Military Engineering, 2014, URL: https://www.uni-nke.hu/document/uni-nke-hu/Bonnyai-Tunde_Doktori-ertekezes_2018.pdf, accessed on 05.02.2021.

EGNOS (European Geostationary Navigation Overlay Service) is also considered to be a European critical infrastructure for Galileo (European satellite navigation system) and Copernicus (the European Union Earth Observation Programme, which monitors our planet and its environment for the benefit of European citizens). On the basis of their objectives, the programmes are specifically designed for civilian purposes.

Eurocontrol (the European Organisation for the Safety of Air Transport) is a Pan-European civil-military intergovernmental organisation established in 1963 to maintain the safety of air traffic services. Eurocontrol and the European Union have concluded a cooperation agreement to implement the Single European Sky. This programme is, in my view, a priority European critical infrastructure.

CERN (European Particle Physics Laboratory) has built the largest scientific measuring equipment for the testing of elementary particles. It pursues the policy of an open society, its research results are public, it is free to visit except for the closed areas, it is free to record buildings everywhere.

The following is a look at the Community protection of the critical infrastructures described above (partially identified in Europe), which covers not only the legal framework but also the realisation of other institutional activities.

3. EU Measures for Critical Infrastructure Protection

A summary of the development history of Critical Infrastructure Protection in Europe is provided by the Handbook on the Protection of Vital Systems and Facilities.[13] As a result of the terrorist act committed in Madrid, on 11 March 2004, the European Commission adopted a Communication on 20 October 2004, entitled *Protecting critical infrastructures in the fight against terrorism*. The Communication made proposals to avoid future terrorist attacks on critical infrastructure, which called for progress in three main areas (prevention, preparedness and response).

On 16 and 17 December 2004, the European Council adopted the European Programme for Critical Infrastructure Protection (EPCIP), presented by the Commission and approved the establishment by the Commission of the Critical Infrastructure Warning Information Network (CIWIN).

EPCIP is designed to ensure a uniform and adequate level of protection for critical infrastructures in the EU. EPCIP needs to be constantly reviewed because it must meet new needs and risks. To ensure these, one must comply with the following principles.

[13] Balázs Bognár, Tünde Bonnyai, Katalin Görög, Lajos Katai-Urban, Gyula Vass, *Létfontosságú rendszerek és létesítmények védelme: kézikönyv a katasztrófavédelmi feladatok ellátására [The protection of the critical systems and infrastructures: manual for disaster management tasks]*, in Nemzeti Közszolgálati Egyetem, Katasztrófavédelmi Intézet, Budapest, 2015.

Subsidiarity, which means that critical infrastructure protection is primarily the responsibility of the Member States, would be focused on European Critical Infrastructures (ECI). It is complementary that the EPCIP framework complements existing measures.

Confidentiality, since critical infrastructure information is extremely important for their operation, makes it much easier to successfully attack them. This principle is also prominent when exchanging information relevant to the protection of critical infrastructures.

According to cooperation between actors, all actors involved in the protection of critical infrastructure (Member States, EU bodies, owners, operators, etc.) should cooperate in the development and implementation of EPCIP in terms of their tasks and responsibilities.

Proportionality principle, according to which defence strategies and measures must be proportionate to the current risk, since it is not realistic to expect all critical infrastructures to be prepared for all hazards, only those which present a real threat to them.

EPCIP consists of three defining workflows. The first is a national framework for the strategy and the development of horizontal measures, the second for the protection of ECIs and the third for helping Member States to protect critical infrastructures.

CIWIN is an emergency alert and security data transmission system that ensures the immediate protection of critical infrastructures and the exchange of best practices in relation to operational incidents. Its main objective is to find innovative and effective tools, methods and procedures in the field of critical infrastructure protection.

It is important to mention the European Reference Network project for the Protection of Critical Infrastructures (ERNCIP), which has been established as an implementation tool for critical infrastructure protection (in particular EPCIP).

On 17 November 2005, the Commission adopted its Green Book on a European programme for the protection of critical infrastructures.[14] The Green Book offered three defence strategies in terms of prevention, preparedness and resilience already defined above; (a) against any threat, (b) protection against all threats, in particular terrorism, and (c) protection against terrorist threats. The Green Paper already contains the five principles (subsidiarity, complementarity, cooperation, confidentiality, proportionality), which are included in Directive 2008/114/EC (Nitra, 2017).

On 8 December 2008, the Council of the European Union adopted (with effect from 12 January 2009) Directive 2008/114/EC (hereinafter "the Directive")

[14] ***, *Green Paper on a European programme for critical infstructure protection*, Commission of the European Communities, Brussels, 2005, p. 2, URL: https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/language-en, accessed on 05.02.2021.

on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. For ease of interpretation, a non-binding guideline has been issued for the application of the Council Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection (EUR 23665 EN, 2008). The guidelines help Member States to derive their data in more detail.

Under the Directive, the measures must be implemented by the Member States within two years of its publication (12 January 2011). A priority for them is to issue annual reports, which should identify the critical infrastructures in the Member States by sector, responsible for designating and identifying them. Every two years, they must submit a summary report covering the vulnerabilities in their area. In addition, Member States have an obligation to inform the Commission of the number of European Critical Infrastructures in their territory designated by sector and of the Member States concerned. The Directive focuses primarily on the energy sector and transport, so these sectoral criteria need to be prioritized. In addition to the sectoral criteria set out in the Directive, Member States are also required to assess critical infrastructure elements on the basis of horizontal criteria.

It notes that there are several infrastructures in the EU that would disrupt or destroy several Member States, and that common minimum rules need to be laid down to remedy them.

According to the definition in the Directive, each operator of critical infrastructure must draw up an operator security plan within one year of designation, which must be reviewed regularly thereafter. It also requires the use of a Security Liaison Officer for designated critical infrastructure and a risk assessment for European Critical Infrastructure located in the territory of the Member States.

The Directive applies to methods of generating and transmitting electricity and to parts of nuclear power plants used for the transmission of electricity, but not to explicit nuclear elements. They are determined by other regulators. In order to comply with the Directive, additional governmental tasks to be implemented by Member States have also been put in place to identify, designate and improve the protection of national critical infrastructures.

The European Council on 25-26 March 2010 adopted the EU Internal Security Strategy at its meeting on the field of critical infrastructure protection, the strategy paid particular attention to the risks posed by modern technologies.

The European Parliament and the Council have adopted Directive 2016/1148 on measures to ensure a uniformly high level of security of network and information systems throughout the Union (NISD). The Directive defines network and information systems as well as the Internet as essential assistance for the free movement of goods, services and persons across borders. The directive states that existing capabilities are not sufficient to guarantee a high level of security of network and information systems in the Union, which requires a global approach. This should include minimum criteria for capacity building and planning, cooperation and exchange of information, and common security requirements for actors.

The following EU organizations provide assistance in critical infrastructure protection.

The EU set up[15] the European Network and Information Security Agency (ENISA) in 2004 to ensure that the EU and its Member States are better prepared to detect, address and prevent information security challenges. The Agency provided practical advice to the EU institutions and to the public and private sectors in the Community in the field of information security. The Agency's remit, as mentioned above, was extended in December 2018 and will continue to operate as the European Network of Experts on EU Network and Information Security, under the name of the European Cyber Security Agency.[16] By performing these tasks, it supports the IT protection of critical infrastructures.

On 1 December 2012, the European Agency for the Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) became operational. The Tallinn-based agency manages the Visa Information System (VIS), the Schengen Information System (SIS II) and the European Fingerprint Identification System (Eurodac) for the security of the Schengen area.[17]

The EUROPOL European Cybercrime Center was set up in 2013[18] to support effective law enforcement action against cybercrime in the EU. Since its inception, it has been involved in a number of high-profile cases, providing on-site assistance for hundreds of successful arrests, and has already scanned hundreds of thousands of files in the course of its analytical work. Each year, it prepares an IOCTA report[19] that includes key findings on cybercrime for the period, as well as new threats.[20] Within the organization, the Focal Point Cyborg unit is responsible for tackling high-tech crimes that primarily threaten critical infrastructures in Europe. EC3's capabilities are also outstanding in the field of forensic informatics, and in its

[15] ***, *Regulation (EC) No 460/2004*, European Parliament and the Council, Brussels, 2004, URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML, accessed on 10.05.2021.

[16] European Union Agency for Cybersecurity, *Homepage*, URL: https://www.enisa.europa.eu/, accessed on 19.02.2021.

[17] European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), *Homepage*, URL: https://eulisa.europa.eu/, accessed on 16.02.2021.

[18] EC3.

[19] ***, *Internet Organised Crime Threat Assessment (IOCTA)*, Europol, Hague, 2020 URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020, accessed on 10.05.2021.

[20] European Cybercrime Centre – EC3, *Homepage*, URL https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, accessed on 16.02.2021.

laboratory set up to support this activity, it also conducts its own IT research and development.

Also established in 2013, the European Council's Cybercrime Program Office (C-PROC) was set up to support the development of cybercrime and electronic evidence legislation in line with the rule of law, and to provide training for judges, prosecutors and law enforcement members. His other responsibilities include promoting cooperation in the field of justice, deepening public-private dialogue, and enhancing international cooperation on cyber security. Protecting children from online sexual violence is a priority for the program office.[21]

From a personal standpoint, it is important to briefly present the Trusted Introducer (TI) service, set up in 2000 and launched by the European CERT community. TI's most important service is to provide a reliable backbone network for event management organizations. Also worth mentioning is the Central European Cyber Security Platform (CECSP), a cyber-security cooperation platform between Hungary, Poland, Austria, the Czech Republic and Slovakia. Finally, it is necessary to get to know the activities of two non-profit organizations; one is the ENCS, established in 2012, to support secure European critical infrastructures, and the other is the European Cyber Security Organization (ECSO), set up in 2016 to represent industry before the European Commission on cyber security.[22]

In the following, I will present the critical infrastructure protection in the Member States and the up-to-date and shortcomings of Community legislation.

4. Member State Critical Infrastructure Protection in Practice

I would like to present the implementation of critical infrastructure protection in the Member States with the measures introduced by Germany. I have chosen this Member State because Berlin is not only a leading power in the European Union, but also a pioneer in the field of Community legislation and harmonization. In addition, it has world-class telecommunications systems, which is also relevant for critical infrastructure, and is the most populous state in Europe.

Since 1990, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) has been coordinating tasks in the field of critical infrastructure protection as an independent body.[23] Its activities are

[21] Cybercrime Programme Office (C-PROC), *Homepage*, URL: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-, accessed on 24.02.2021.

[22] Zoltán Kovács, "Kibervédelem és biztonság", [Cyber protection and security], in *Kibervédelem a bűnügyi tudományokban*, Ludovika Egyetemi Kiadó Nonprofit Kft. – Ludovika Press, Budapest, pp. 65-90.

[23] Federal Office for Information Security, Germany, Homepage, URL: https://www.bsi.bund.de/EN/Home/home_node.html accessed on 27.04.2021.

supported by the National Cyber-Abwehrzentrum (NCAZ), established in line with the 2011 strategy, whose main task is to establish operational-level cooperation between government agencies in the event of major IT incidents. In addition to its other important functions, it also carries out national management and analysis center activities. A number of other organizations also help protect critical infrastructure, such as the Federal Office for Civil Protection and Disaster Management (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK). These include, but are not limited to cyber security, the National Cyber Security Council (Nationaler Cyber-Sicherheitsrat), the Federal Government Commissioner for Information Technology (Beauftragter der Bundesregierung für Informationstechnik), the Cyber Security Association (Allianz), Allianz Information Technology Situation Center (Nationales IT-Lagezentrum) and several CERTs (Event Management Centers) in Germany.[24] All this shows that the creation of a complex protection and organizational system in the field of critical infrastructure protection is one of the key issues in terms of effectiveness.

In addition to setting up a number of organizations and institutions, Germany has also taken significant steps in other areas, as it has created its Digital Strategy, which covers the period between 2015-2025. Mention should also be made of the Digital Agenda, which was in force for the period between 2014-2017. This was preceded by the National Critical Infrastructure Protection Strategy dated 2009[25] and the 2011 Cyber Security Strategy, which can be classified as first generation strategies, so their primary goal was to build online trust. This strategy has been replaced by the new Cyber Security Strategy of 2016, as a second-generation strategy, in which a holistic approach has already been taken, so that it covers all security sectors, especially critical infrastructures. In addition, the German constitution states that the state must guarantee security for and provide basic care to the population, which implies a critical role in critical infrastructure protection. These documents show that Germany is taking significant steps with regard to infrastructure protection, not only in its organizational system, but also in codification and in shaping its day-to-day security policy.

In 2001, Germany considered terrorism to be the most important risk in terms of critical infrastructure protection. Since then, various cyber threats have become priorities that can come from multiple directions. This risk has been exacerbated by the D21 initiative, which aims to encourage Germany's transformation from an

[24] Dóra Molnár, "Kiberbiztonság Németországban – pillanatkép a német digitális térről" [Cyber security in Germany – a snapshot of the German digital space], in *Nemzet és Biztonság,* 2018/1. szám, pp. 142–156.

[25] Federal Republic of Germany, Federal Ministry of the Interior, *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Berlin, 2009, URL: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1, accessed on 27.04.2021.

industrial society to an information society. In 2003, the country involved utilities in the protection of the area, which helped clarify the definition environment, and in addition to rethinking previous sectors, nine sectors were named (energy, health, state and administration, food, transport and transportation, finance and transport, IT and telecommunications, media and culture, water).[26] It is an important fact that ninety percent of critical infrastructures are privately owned, which is why the government, through the organizations named above, has an effective monitoring and intervention role in place, which must be maintained in the future. Building on the experience of the last ten years, Germany sees critical infrastructure protection as a cornerstone of its internal security. Measures have been implemented to support this and a number of pieces of legislation have entered into force. With the increasing use of information technology, the application of new innovative technologies, such as AI, raises huge expectations, but at the same time generates new dependencies that need to be minimized. International terrorism and the growing impact of climate change are also seen as a global challenge.[27]

This chapter presents the complexity of the legislation and series of measures that Member States had to implement in addition to Community legislation and measures in order to achieve effective infrastructure protection. This part of the study justifies, in my view, the need for the EU to rethink its existing regulations in the field of critical infrastructure protection.

Conclusions

In this study, the risks to critical infrastructures were presented, followed by the sectors and their main characteristics, as well as a few key European critical infrastructures. Afterwards, it was illustrated the EU's action in the field of critical infrastructure protection, which also described Common procedures. Furthermore, we considered it important to present the measures taken by the Member States, most notably Germany, as the EU has left the majority of the regulation of critical infrastructure to the Member States. In conclusion, attacks on a number of critical infrastructures around the world have demonstrated the vulnerability of open societies. These societies view their security not in the success of regular warfare but in the smooth running of their daily lives. The European Union, and thus their

[26] Bundesministerium des Innern, *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, [Protection of critical infrastructures – Risk and Crisis Management]*, Berlin, 2011, p. 8, URL: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/bmi_schutz_kritis_risiko_und_krisenmanagement.pdf?__blob=publicationFile&v=8, accessed on 27.04.2021.

[27] Bundesministerium des Innern, *10 Jahre „KRITIS-Strategie*, [10 years, "KRITIS strategy], Berlin, 2020, p. 89, URL: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-21-zehn-jahre-kritis-strategie.pdf?__blob=publicationFile&v=7, accessed on 29.08.2021.

Member States, consider the key to their economic development to be secured in the future by moving from industrial societies to information societies. However, this direction has enhanced the effectiveness of critical infrastructure protection, whose sectors are indispensable in creating and maintaining the desired digital environment. Changing Russia's military doctrine, one of the biggest security challenges for the EU, and putting it into practice is a successful model that hybrid warfare in Ukraine has shown very clearly. Here, a number of attacks have hit critical infrastructure sectors that have not been adequately prepared for these actions, causing significant detriment to regular military operations. Hybrid warfare can otherwise be seen as an analogy to the Cold War and should be seen as a longer-term risk. As a result, the cyber dimension of critical infrastructures is becoming increasingly important for modern industrial/digital societies. This is why critical infrastructures need the most outstanding protection against IT attacks. The events in Ukraine have also shown the extent to which attacks on critical infrastructure can cause economic damage at the national level, so the regional impact of possible attacks on identified European critical infrastructures must be taken into account. In examining Community legislation and measures, I have come to the view that the EU should review its rules on critical infrastructure (e.g. sectoral allocation) and add new elements in the light of changed foreign policy dimensions and cyber threats. Member States can make progress in this area to varying degrees (depending on their economic strength), but the interdependence of critical infrastructures and the threat of the domino principle call for uniform, strong action in this area. Account should also be taken of the fact that the majority of owners/operators of critical infrastructures can be linked to private capital and, as security requires a significant financial outlay, optimization in the field of security is not allowed. For this reason, the bodies of the European Union and the authorities of the Member States must continue to play an effective monitoring and enforcement role in this area.

BIBLIOGRAPHY:

1. ALEXANDRU, Adriana; VEVERA, Victor; CIUPERCĂ, Ella Magdalena, "National Security and Critical Infrastructure Protection", in *International Conference Knowledge-Based Organization*, Vol. XXV, No. 1/2019.

2. BARTOS Aleksandr, "Гибридная война – новый вызов национальной безопасности России, [Hybrid war is a new challenge to Russia's national security]", in *НеЗавнспmoe*, URL: http://www.nationaldefense.ru/includes/periodics/maintheme/2017/1016/154222573/detail.shtml

3. BARTOS Aleksandr, "Гибридная война – переход от неудач к победе [Hybrid warfare – Transition from Failure to Victory]", in *НеЗавнспmoe*, https://nvo.ng.ru/realty/2018-06-01/1_998_hybryd.html

4. BARTOS Aleksandr, "Россия в эпоху гибридных войн [Russia in the era of hybrid wars]", in *Не3абнcnmое*, URL: http://nvo.ng.ru/gpolit/2017-10-20/1_970_hybrid.html

5. BOGNÁR, Balázs; BONNYAI, Tünde; GÖRÖG, Katalin; KATAI-URBAN, Lajos; VASS, Gyula, *Létfontosságú rendszerek és létesítmények védelme: kézikönyv a katasztrófavédelmi feladatok ellátására [The protection of the critical systems and infrastructures: manual for disaster management tasks]*, in Nemzeti Közszolgálati Egyetem, Katasztrófavédelmi Intézet, Budapest, 2015.

6. BONNYAI, Tünde, *A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében [Analysis of the critical infrastructure protection in the light of population training]*, in Doktori (PhD) Értekezés, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, 2014.

7. Bundesministerium des Innern, *10 Jahre "KRITIS-Strategie"* [10 years, „KRITIS strategy], Berlin, 2020, URL: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-21-zehn-jahre-kritis-strategie.pdf?__blob=publicationFile&v=7

8. Bundesministerium des Innern, *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement,* [Protection of critical infrastructures – Risk and Crisis Management], Berlin, 2011, URL: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/bmi_schutz_kritis_risiko_und_krisenmanagement.pdf?__blob=publicationFile&v=8

9. Commission Of The European Communities, *Green Paper on a European programme for critical infstructure protection*, Brussels, 2005, URL: https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/language-en

10. European Parliament And The Council, *Regulation (EC) No 460/2004*, Brussels, 2004, URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

11. ***, *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Federal Republic Of Germany, Federal Ministry of the Interior, Berlin, 2009.

12. HORVÁTH, Attila, "A létfontosságú rendszerelemek és a technológiai fejlődés új kockázatai II. Rész", [New Risks of Critical Infrastructure and Technological Development. Part II.], in *Hadtudomány*, electronic issue, 2016, URL: http://mhtt.eu/hadtudomany/2016/2016_elektronikus/horvathattila22.pdf

13. JÓJÁRT, Krisztián, "A hibrid hadviselés orosz elméletének változása az ukrajnai tapasztalatok tükrében" [The change of the Russian hybrid warfare's theory in the light of the Ukrainian experiences], in *Hadtudomány*, no. 1-2/2019.

14. KOVÁCS Zoltán, "Kibervédelem és biztonság", [Cyber protection and security], in *Kibervédelem a bűnügyi tudományokban*, Ludovika Egyetemi Kiadó Nonprofit Kft., Ludovika Press, Budapest.

15. MARAZIS, Andreas; KOTHE, Rober, "Russian Cyberwarfare Capabilities: Assessing the Threat for Ukraine's Critical Infrastructure", in *European Neighbourhood Council Analysis*, 2018.

16. MOLNÁR, Dóra, "Kiberbiztonság Németországban – pillanatkép a német digitális térről" [Cyber security in Germany - a snapshot of the German digital space], in *Nemzet és Biztonság*, no. 1/2018.

17. RINALDI, S.M.; PEERENBOOM, J.P.; KELLY, T.K., "Identifying, understanding, and analyzing critical infrastructure interdependencies", in *IEEE Control Systems Magazine*, vol. 21, no. 6, 2001.

18. TRENIN, Dmitri, "Avoiding U.S.–Russia Military Escalation During the Hybrid War", in *Carnegie Moscow*, URL: https://carnegie.ru/2018/01/25/avoiding-u.s.-russia-military-escalation-during-hybrid-war-pub-75277

19. VIRGIL, Toma, "Evoluția conceptului de infrastructură critică", [The evolution of the concept of critical infrastructure], in *Inspectoratul pentru Situații de Urgență al Județului Argeș*, URL: http://www.igsu.ro/documente/publicatii/articole_de_specialitate/Evolutia_conceptului_de_infrastructura_critica.pdf

20. WHITEHEAD, David E.; OWENS, Kevin; GAMMEL, Dennis; SMITH, Jess, "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies", in *Power and Energy Automation Conference*, Spokane, Washington, 2017.