SFT VOL. 57 ISSUE 1, 2021, PP. 50–62

Rafał Wróbel[a)*], Ilona Kinga Wróbel

[a)] *The Main School of Fire Service / Szkoła Główna Służby Pożarniczej*
[*] *Corresponding author / Autor korespondencyjny: rwrobel@sgsp.edu.pl*

Critical Infrastructure in Poland during the COVID-19 Pandemic

Infrastruktura krytyczna w Polsce w warunkach pandemii COVID-19

ABSTRACT

Purpose: The paper presents the results of the review of literature and of the legal regulations in the field of the protection of critical infrastructure in Poland during the COVID-19 pandemic. The assumed main goal was to determine the requirements for protecting elements catalogued in 11 critical infrastructure systems, in the face of the risk of losing key personnel and the need to maintain continuity of critical infrastructure operations.
Introduction: The first part of the paper discusses the essence and methods of identifying critical infrastructure in Poland. Further on, possible clauses were identified of an epidemic and its impact on individual critical infrastructure systems, with particular focus on the fact that if an epidemic occurs, there may be a temporary or long-term shortage of personnel essential to the business continuity of the facilities, installations and elements included in critical infrastructure. Then, the legal solutions for maintaining the operating continuity of critical infrastructure during COVID-19 implemented in 2020 were presented, pointing to legal tools aimed at ensuring the resilience of critical infrastructure by securing key resource, i.e. the employees.
Methodology: Literature research and qualitative analysis were carried out of the legal acts announced in 2020 related to enhancing the resilience of critical infrastructure, and a review was carried out of the recommendations and guidelines addressed to critical infrastructure operators, which were issued in March and September of 2020. The obtained results were analysed using the following: publications, acts of the Polish law, recommendations and guidelines published on the websites of governmental institutions, interviews with independent experts.
Conclusions: The first regulations on specific arrangements meant to prevent, counteract and combat COVID-19, other contagious diseases and crisis situations caused by them did not contain any provisions that would be supportive of the protective capacity of the critical infrastructure elements in Poland. The first document in this respect, RCB guidelines of 16 March 2020 have not been formalised yet in the legal system. The so-called Shield 2.0 of 31 March 2021 introduced to the 15x of the COVID-19 Act the tools for specific employers entitled to take advantage of new, previously unavailable opportunities to ensure the continuity of services. Those entitlements made it possible to change the work system or work schedule of employees, to instruct them to work overtime, as well as to refuse to grant annual leave or to cancel it.
Keywords: critical infrastructure, pandemic, COVID-19, law, key personel
Type of article: case study

Received: 08.06.2021; Reviewed: 28.06.2021; Accepted: 28.06.2021;
Authors` ORCID IDs: R. Wróbel – 0000-0002-2338-0267; I. K. Wróbel – 0000-0002-8869-5657
The authors contributed the equally to this article;
Please cite as: SFT Vol. 57 Issue 1, 2021, pp. 50–62, https://doi.org/10.12845/sft.57.1.2021.4;

ABSTRAKT

Cel: W artykule przedstawiono wyniki analizy literatury przedmiotu oraz przepisów prawa w zakresie ochrony infrastruktury krytycznej w Polsce w warunkach pandemii COVID-19. Za cel główny przyjęto zdefiniowanie uwarunkowań ochrony elementów skatalogowanych w jedenastu systemach infrastruktury krytycznej wobec ryzyka utraty kluczowego personelu oraz konieczności utrzymania ciągłości działania infrastruktury krytycznej.
Wprowadzenie: W pierwszej części artykułu przybliżono istotę oraz sposób identyfikacji infrastruktury krytycznej w Polsce. W dalszej części zidentyfikowano możliwe przyczyny powstania epidemii oraz określono jej wpływ na poszczególne elementy systemu infrastruktury krytycznej (IK) zwracając szczególną uwagę na fakt, że wraz z wystąpieniem epidemii możliwa jest chwilowa lub długotrwała utrata personelu istotnego dla zapewnienia ciągłości działania obiektów, instalacji i elementów wchodzących w skład systemów IK. Następnie zaprezentowano rozwiązania prawne na rzecz utrzymania ciągłości działania IK w warunkach COVID-19 zaimplementowane w 2020 roku, wskazując na narzędzia prawne mające na celu zapewnienie odporności infrastrukturze krytycznej poprzez zabezpieczenie kluczowego zasobu, jakim są pracownicy.

Metodologia: Przeprowadzono badania literatury przedmiotu oraz dokonano analizy jakościowej ogłoszonych w 2020 roku aktów prawnych w zakresie zwiększania odporności IK oraz przestudiowano rekomendacje, zalecenia i wytyczne wydane w marcu oraz wrześniu 2020 roku skierowane do operatorów IK. Do analizy przeprowadzonych badań wykorzystano publikacje zwarte, akty prawa polskiego, zalecenia i wytyczne ogłaszane na stronach instytucji rządowych, wywiady z niezależnymi ekspertami.
Wnioski: Początkowe wytyczne dotyczące szczególnych rozwiązań związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych nie zawierały zapisów wzmacniających możliwości ochronne elementów IK w Polsce. Pierwszy dokument w tym zakresie, wytyczne RCB z 16 marca 2020 r., nie zostały sformalizowanie w systemie prawa. Dopiero Tarcza 2.0 z dnia 31 marca 2021 r. wprowadziła w formule 15x ustawy w sprawie COVID-19 narzędzia dla określonych pracodawców uprawnionych do skorzystania z nowych, dotychczas niedostępnych możliwości zapewnienia ciągłości usług. Wspomniane uprawnienia umożliwiły zmianę systemu albo rozkładu pracy pracowników, wydawanie im polecenia pracy w ramach godzin nadliczbowych (tzw. nadgodziny), jak również odmowę udzielenia urlopu albo jego odwołania.
Słowa kluczowe: infrastruktura krytyczna, pandemia, COVID-19, prawo, kluczowy personel
Typ artykułu: studium przypadku

Przyjęty: 08.06.2021; Zrecenzowany: 28.06.2021; Zaakceptowany: 28.06.2021;
Identyfikatory ORCID autorów: R. Wróbel – 0000-0002-2338-0267; I. K. Wróbel – 0000-0002-8869-5657;
Autorzy wnieśli równy wkład merytoryczny w powstanie artykułu;
Proszę cytować: SFT Vol. 57 Issue 1, 2021, pp. 50–62, https://doi.org/10.12845/sft.57.1.2021.4;

Introduction

Poland, like other countries worldwide, is protecting the key aspects of the state activity as an entity, which enable the implementation of functions defined by the Constitution of the Republic of Poland, including guaranteeing widely understood security of the citizens. Legal conditions set out in different time periods define principles for the protection of elements, including infrastructure, which are of key importance for ensuring security [1–2]. They apply, among others, to:

- facilities of particular importance for state security and defence,
- areas, facilities and equipment subject to mandatory protection,
- equipment, facilities, installations, services of key importance for security of the state and its citizens necessary to ensure effective functioning of public administration bodies, as well as institutions and entrepreneurs.

It is the latter ones which, according to Act of 26 April 2007 on crisis management, define critical infrastructure. It should be noted that even though the concept of critical infrastructure was formalised for the first time in Polish legal regulations in 2007, it was defined earlier, both in literature of the subject or at the occasion of involving the National Security Bureau in discussions concerning protection of critical infrastructure under NATO (the North Atlantic Treaty) [3]. Critical infrastructure has been identified in the list divided into systems. Initially there were nine systems, but finally eleven systems determined. Critical infrastructure includes the following systems [4]:

- energy supply, energy raw materials and fuels,
- communications,
- telecommunication,
- financial,
- provision of food,

Wprowadzenie

Polska – podobnie jak inne kraje na świecie – chroni kluczowe aspekty działalności państwa jako podmiotu, które umożliwiają realizację funkcji zdefiniowanych w Konstytucji RP oraz służą zapewnieniu szeroko rozumianego bezpieczeństwa obywateli. Ustalone w różnych okresach czasu uwarunkowania prawne definiują zasady ochrony elementów kluczowych (w tym infrastruktury) dla zapewnienia bezpieczeństwa [1–2]. Odnoszą się one m.in. do:

- obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa,
- obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie,
- urządzeń, obiektów, instalacji, usług kluczowych dla bezpieczeństwa państwa i jego obywateli oraz służących zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

To właśnie te ostatnie, zgodnie z ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, definiują infrastrukturę krytyczną. Należy odnotować, że pojęcie infrastruktury krytycznej, choć sformalizowane po raz pierwszy w przepisach prawa w Polsce w 2007 r., definiowane było już wcześniej – czy to w literaturze przedmiotu, czy też przy okazji zaangażowania Biura Bezpieczeństwa Narodowego w dyskusję na temat ochrony infrastruktury krytycznej w ramach Traktatu Sojuszu Północnoatlantyckiego, tj. NATO [3]. Infrastruktura krytyczna została sporządzona w formie wykazu z podziałem na systemy. Początkowo można było wyróżnić dziesięć, ale ostatecznie sformułowano jedenaście systemów. Infrastruktura krytyczna obejmuje systemy [4]:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności,
- sieci teleinformatycznych,
- finansowe,

- water supply,
- health protection,
- transport,
- rescue,
- system assuring operational continuity of public administration,
- systems of production, storage and usage of chemical and radioactive substances, including hazardous substances line.

It was possible to identify critical infrastructure due to two types of criteria developed, applied (the criteria are used in the identification of elements of the critical infrastructure list and during its regular updates) and protected ones – classified Part of the National Programme for Critical Infrastructure Protection [5]. The first type – system criteria – and refers to the function of a potential element (facility, equipment, installation or service) of the critical infrastructure, assigned to a given system (and to be more precise to a specific sector within the system). The second type – cross-sectional criteria – specifies the parameters necessary to determine the effect of the dysfunction (destruction or non-functioning) of a potential element of critical infrastructure. The cross-sectional nature of the above-mentioned element is analysed on 7 levels (according to the National Critical Infrastructure Protection Program 2020. The cross-sectional criteria include: human casualties (1), financial consequences (2), necessity to evacuate (3), loss of service (4), restoration time (5), international effect (6), uniqueness (7). If, after meeting the systemic criterion and the definitional criterion, at least two of the seven cross-sectional criteria are achieved, the criterion is considered to be met and the analysed element is considered as critical infrastructure. From the formal viewpoint, the identification of the individual elements of critical infrastructure is referred to as establishing a list [6, p. 40–41]. This determination takes place via a resolution adopted by the Council of Ministers. Extracts are drawn from the list adopted in that form and in accordance with the rules on the protection of classified information they are turned over to coordinators of critical infrastructure systems (extracts for each of the systems) and provincial governor (extracts for each province). The list of critical infrastructure is regularly updated in a way similar to mentioned above.

The number of critical infrastructure elements in individual systems is highly diversified. Regardless of this, the responsibility – of both the coordinators of individual systems and of the operators – is defined according to the principle of equal treatment. The primary responsibility for the protection of critical infrastructure lies in the first place with its operator, who develops, agrees and submits for approval a plan of protection for critical infrastructure, yet such an operator may also gain support from the public administration, and may jointly form a promoted relation of public-private partnership. The critical infrastructure protection plan covers risks to the critical infrastructure, as well as measures to be undertaken if a given type of hazard or disruption in the functioning of critical infrastructure occurs. One of the hazards which is clearly taken into consideration is an epidemic and its pecific type – a pandemic.

- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowy,
- ratowniczy,
- zapewniający ciągłość działania administracji publicznej,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągów substancji niebezpiecznych.

Identyfikacja infrastruktury krytycznej była możliwa dzięki dwóm rodzajom kryteriów wypracowanych, wykorzystywanych (w procesie identyfikacji elementów wykazu infrastruktury krytycznej i w czasie jego regularnie dokonywanej aktualizacji) oraz chronionych – zapisanych w niejawnym załączniku do Narodowego Programu Ochrony Infrastruktury Krytycznej [5]. Pierwszy rodzaj – kryterium systemowe – odnosi się do funkcji potencjalnego elementu (obiektu, urządzenia, instalacji lub usługi) infrastruktury krytycznej, przypisanej do danego systemu (a dokładniej do określonego sektora w ramach systemu). Drugi rodzaj – kryterium przekrojowe – podaje parametry umożliwiające określenie skutków dysfunkcji (zniszczenia albo zaprzestania funkcjonowania) potencjalnego elementu infrastruktury krytycznej. Przekrojowy charakter ww. elementu jest rozpatrywany na siedmiu płaszczyznach. Zgodnie z Narodowym Program Ochrony Infrastruktury Krytycznej 2020. Kryteria przekrojowe obejmują: ofiary w ludziach (1), skutki finansowe (2), konieczność ewakuacji (3), utratę usługi (4), czas obudowy (5), efekt międzynarodowy (6), unikatowość (7). W sytuacji, gdy po spełnieniu kryterium systemowego oraz kryterium definicyjnego, co najmniej dwa z siedmiu kryteriów przekrojowych zostaną osiągnięte, kryterium uznaje się za spełnione i rozpatrywany element jest uznawany za infrastrukturę krytyczną. Z formalnego punktu widzenia ustalenie elementów infrastruktury krytycznej określa się mianem ustalenia wykazu [6, s. 40–41]. Owo ustalenie następuje w drodze uchwały podejmowanej przez Radę Ministrów. Z przyjętego w opisanej formie wykazu sporządzane są wyciągi, które – z zachowaniem przepisów o ochronie informacji niejawnych – przekazywane są koordynatorom systemów infrastruktury krytycznej (wyciągi dla każdego z systemów) oraz wojewodom (wyciągi dla każdego z województw). Wykaz infrastruktury krytycznej podlega regularnej aktualizacji w trybie analogicznym do opisanego wyżej.

Liczba elementów infrastruktury krytycznej w poszczególnych systemach jest bardzo zróżnicowana. Niezależnie od tego odpowiedzialność – zarówno koordynatorów poszczególnych systemów, jak i samych operatorów – jest definiowana w oparciu o zasadę równego traktowania. Zasadnicza odpowiedzialność za ochronę infrastruktury krytycznej w pierwszej kolejności spoczywa na jej operatorze. Do jego zadań należy opracowanie, uzgodnienie i przedłożenie do zatwierdzenia planu ochrony infrastruktury krytycznej. Ma on również swego rodzaju możliwość uzyskania wsparcia od administracji publicznej, tworzącej z nim zalecaną relację partnerstwa publiczno-prywatnego. Plan wskazuje zagrożenia dla infrastruktury krytycznej, jak również działania w sytuacji zagrożenia określonego rodzaju lub zakłócenia funkcjonowania infrastruktury krytycznej. Jednym z często pojawiających się zagrożeń jest epidemia oraz jej szczególna forma, czyli pandemia.

Impact of epidemic on critical infrastructure systems

Epidemics pose a direct threat to human beings – frequently underestimated, but also a key element in the operation of critical infrastructure systems.

Epidemics of infectious diseases, including influenza, can occur all over the country. The catastrophic effects of the epidemic tend to spread primarily in areas of large human clusters, such as: schools, kindergartens, public utility facilities, major industrial plants, as well as public transport centres (airports, railway stations, subway stations), as well as individual means of public transport.

The main causes of outbreaks of epidemics include, among others:

- unintentional introduction of a pathogen (bacteria, viruses),
- effects of other catastrophic events such as floods,
- failure to comply with certain sanitary, hygienic and veterinary requirements,
- bringing the illness from areas outside the country,
- bioterrorism.

In the vulnerability of critical infrastructure to risks, the human factor should also be taken into account as an internal factor of susceptibility to risks.

The determination of the consequences of an epidemic includes [7]:

- directly affected population (the number of fatalities and the number of hospitalisations),
- number of evacuees/persons isolated,
- number of people who have lost access to basic services.

The occurrence of an epidemic may result primarily in [7]:

- a direct threat to human life and health (including also indirectly due to inefficiency of the healthcare system and/or social care system),
- the possible need for hospitalisation/isolation of people,
- temporary difficulties in travelling within the country and abroad,
- difficulties in accessing food and potable water,
- the possibility of "panic" among the population and a threat of disturbing public order,
- a possible increase in criminal offences and an uptrend in the number of common crimes and offences (burglary, robbery, destruction of property).

Possible effects on critical infrastructure systems are shown in Figure 1.

Wpływ epidemii na systemy infrastruktury krytycznej

Epidemie zagrażają bezpośrednio człowiekowi, który jest istotnym i często niedocenianym elementem funkcjonowania systemów infrastruktury krytycznej.

Epidemie chorób zakaźnych, w tym grypy, mogą wystąpić na terenie całego kraju. Katastrofalne skutki epidemii rozprzestrzeniają się przede wszystkim w miejscach dużych skupisk ludzkich, takich jak: szkoły, przedszkola, miejsca użyteczności publicznej, duże zakłady przemysłowe, a także w centrach komunikacji publicznej (lotniska, dworce, stacje metra), jak i poszczególnych środkach transportu publicznego.

Do głównych przyczyn wystąpienia epidemii zalicza się m.in.:

- nieświadome wprowadzenie czynnika patogennego (bakterie, wirusy),
- skutki innych zdarzeń katastroficznych, takich jak powodzie,
- niezachowanie określonych wymogów sanitarno-higienicznych i weterynaryjnych,
- zawleczenie choroby z obszarów leżących poza granicami kraju,
- bioterroryzm.

W przypadku podatności infrastruktury krytycznej na zagrożenia należy uwzględnić również aspekt ludzki jako wewnętrzny czynnik podatności na zagrożenia.

Określenie skutków wystąpienia epidemii obejmuje [7]:

- ludność bezpośrednio poszkodowaną (liczbę zachorowań śmiertelnych i liczbę hospitalizowanych),
- liczbę ewakuowanych/izolowanych,
- liczbę ludzi, którzy utracili dostęp do podstawowych usług.

Wystąpienie epidemii może skutkować przede wszystkim [7]:

- bezpośrednim zagrożeniem dla życia i zdrowia osób (w tym również pośrednio w wyniku niewydolności systemu opieki zdrowotnej i/lub systemu opieki społecznej),
- możliwą koniecznością hospitalizacji/izolacji ludności,
- okresowymi utrudnieniami w przemieszczaniu się po terenie kraju, jak i zagranicą,
- utrudnieniami w dostępie do żywności i wody pitnej,
- możliwością wystąpienia paniki wśród ludności oraz zagrożeniem zakłócenia porządku publicznego,
- możliwym wzrostem przestępczości o charakterze kryminalnym oraz zwiększoną liczbą przestępstw i wykroczeń pospolitych (kradzieże z włamaniem, rozboje, niszczenie mienia).

Możliwe skutki dla systemów infrastruktury krytycznej zaprezentowano na rycinie 1.

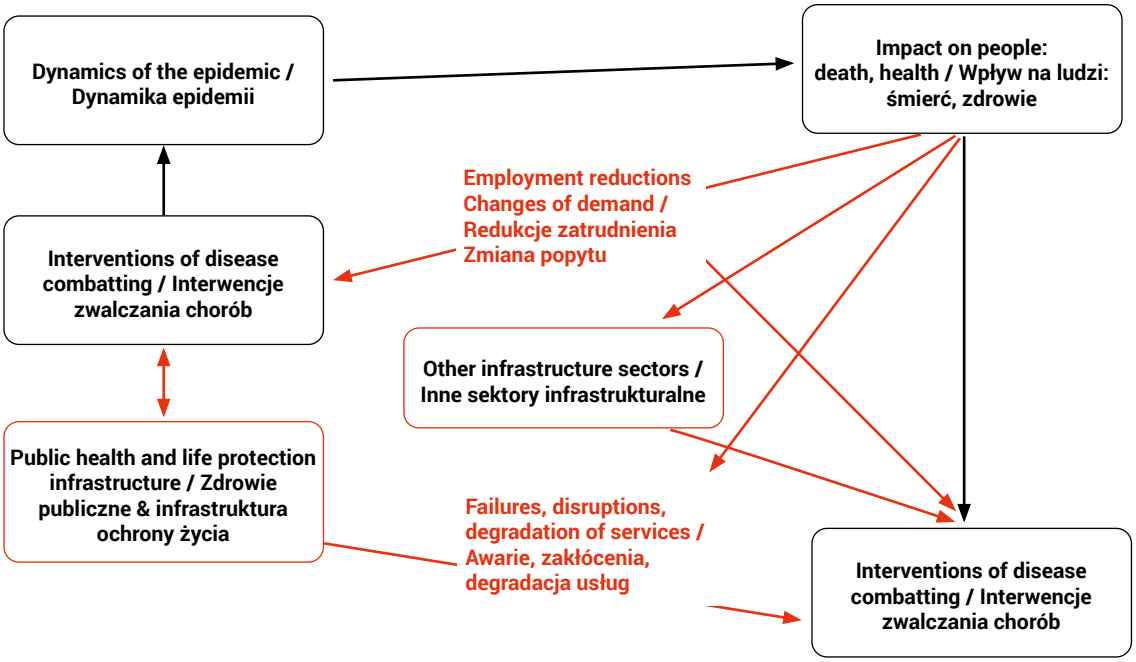

Figure 1. The effects of an epidemic threst on critical infrastructure
Rycina 1. Skutki zagrożenia epidemicznego dla infrastruktury krytycznej

Source: Own elaboration.
Źródło: Opracowanie własne.

From the point of view of 11 critical infrastructure systems, it seems that the healthcare system is the most vulnerable to disruptions caused by an outbreak of an epidemic.

The main problems that may arise under this system are as follows [9]:

- a disproportionate number of patients as compared to the capacity of the whole system,
- shortage of medical staff and equipment,
- shortages of medicines, vaccines and personal protective equipment,
- disruptions in the operation of healthcare facilities, resulting from the panic of the society, as well as the expected absence among healthcare employees,
- logistics problems due to stock-outs, or problems related to transport,
- problems caused by a high number of deaths,
- general practitioners may have 100 new patients per 100 000 people per week, and during the epidemic peak as many as 250 patients per 100 000 people per week – taking into account patients with complications, the number of new patients in the epidemic peak could be as high as 500 patients/week. This is of great importance, especially for individual practices [10, p. 102].

The potential consequences of an epidemic may also affect the remaining critical infrastructure systems and may directly come down to:

- inducing morbidity and/or mortality among employees handling critical infrastructure,

Spośród jedenastu wspomnianych wyżej systemów infrastruktury krytycznej najbardziej podatnym na zakłócenia spowodowane wybuchem epidemii bez wątpienia jest system ochrony zdrowia.

Podstawowe problemy, jakie mogą wystąpić w ramach przywołanego systemu to [9]:

- nieproporcjonalnie duża liczba pacjentów w porównaniu do możliwości całego systemu,
- niedobór personelu i sprzętu medycznego,
- niedobór leków, szczepionek i środków ochrony indywidualnej,
- zaburzenia w funkcjonowaniu placówek służby zdrowia, wynikające z paniki społeczeństwa, a także spodziewanej absencji wśród pracowników ochrony zdrowia,
- problemy logistyczne związane z wyczerpaniem zapasów, czy też problemy związane z transportem,
- problemy wynikające z dużej liczby zgonów,
- lekarze rodzinni mogą mieć 100 nowych pacjentów na 100 000 populacji na tydzień, a podczas szczytu epidemii nawet 250 pacjentów na 100 000 populacji na tydzień – uwzględniając pacjentów z powikłaniami. Liczba nowych pacjentów w szczycie epidemii może osiągnąć nawet 500 pacjentów/tydzień. Ma to ogromne znaczenie, szczególnie dla praktyk prowadzonych indywidualnie [10, s. 102].

Potencjalne skutki epidemii mogą wywierać wpływ również na pozostałe systemy infrastruktury krytycznej i przyczynić się bezpośrednio do:

- wywołania zachorowań i/lub zgonów wśród pracowników obsługujących infrastrukturę krytyczną,

- economic and commercial losses,
- destabilisation of social and political structures,
- uncontrolled increase in the costs of the epidemic (consequences for the financial system),
- impact on the economy at a regional and national level (e.g. changes in interest rates, drops in the exchange rate or stock exchange quotes),
- disruptions in the functioning of the whole economy due to the absence of staff of enterprises and institutions, facilities, equipment or systems of which constitute the critical infrastructure,
- possible economic crisis and a significant drop in GDP resulting from the isolation of considerable areas,
- long-term blockage of traffic routes/hubs causing immobilisation or difficulties in transport or communication;
- blockades within intra-EU trade and exports,
- the necessity for large expenditure from the state budget related to the elimination of the consequences of the event.

There is a general consensus that a potential temporary or long-term loss of staff crucial for assuring the operating continuity of facilities, systems and installations comprised by those systems is a critical risk (perhaps even the most serious one) to all critical infrastructure systems arising from the occurrence of an epidemic.

Legal solutions to maintain the continuity of functioning of critical infrastructure during COVID-19 epidemic

The functioning of the critical infrastructure is indispensable when responding to a crisis caused by COVID-19 in the health protection sector, and one that puts a widely understood social security and well-being at risk. When taking actions aimed at stopping the spread of the virus, securing the functioning continuity of the critical infrastructure was correctly recognised as a priority. Taking this into account, on 16 March 2020, i.e. less than two weeks after the first cases of COVID-19 were recorded in Poland, "The guidelines for operators of critical infrastructure on preventive measures aimed at preventing the spread of the SARS-CoV-2 coronavirus" were issued [11]. The guidelines comprised of recommendations for the operators (owners) of critical infrastructure facilities, and specified rules for ensuring safe working conditions, e.g. through:

- executing information and educational campaigns among staff members related to transmission of SARS-CoV-2 virus, incubation time and the symptoms to be expected, rules to be followed to limit the risk of contracting the virus, including also the recommended individual preventive means,
- making changes in work organisation and providing additional safety measures, such as introducing remote work, limiting contacts between the employees, changing rules for having meals, limiting the entry and exit points, introducing mandatory hand disinfection and

- strat ekonomicznych i handlowych,
- destabilizacji struktur społecznych i politycznych,
- niekontrolowanego przyrostu kosztów wystąpienia epidemii (skutki dla systemu finansowego),
- negatywnego wpływu na gospodarkę na poziomie regionalnym i krajowym (np. zmianę stóp procentowych, spadki kursu waluty lub notowań giełdy),
- zakłóceń w funkcjonowaniu całej gospodarki wynikających z nieobecności kadry przedsiębiorstw i instytucji, których obiekty, urządzenia lub instalacje stanowią infrastrukturę krytyczną,
- możliwego kryzysu ekonomicznego i znacznego spadku PKB związanego z izolacją znacznych terenów,
- długoterminowego zablokowania szlaków/węzłów komunikacyjnych powodujących unieruchomienie lub utrudnienia w transporcie, czy też utrudnień komunikacyjnych,
- blokad w obrębie handlu wewnątrzunijnego i eksportu,
- konieczności poniesienia dużych nakładów z budżetu państwa związanych z likwidacją skutków zdarzenia.

Istnieje zgodność co do tego, że być może najpoważniejszym zagrożeniem dla wszystkich systemów infrastruktury krytycznej, wynikającym z wystąpienia epidemii, jest możliwa chwilowa lub długotrwała utrata personelu istotnego dla zapewnienia ciągłości działania obiektów, instalacji i elementów wchodzących w skład tychże systemów.

Rozwiązania prawne na rzecz utrzymania ciągłości działania infrastruktury krytycznej w warunkach COVID-19

Właściwe funkcjonowanie infrastruktury krytycznej jest niezbędne podczas reagowania na kryzys związany z COVID-19 w sektorze ochrony zdrowia, zagrażający szeroko rozumianemu bezpieczeństwu i dobrobytowi społeczeństwa. Podejmując działania mające na celu zatrzymanie rozprzestrzeniania się wirusa, słusznie jako priorytet została określona kwestia zabezpieczenia ciągłości funkcjonowania infrastruktury krytycznej. Biorąc powyższe pod uwagę, już 16 marca 2020 (a zatem niecałe dwa tygodnie od pojawiania się pierwszych przypadków zachorowań na COVID-19 w Polsce) wydane zostały „Wytyczne dla operatorów infrastruktury krytycznej w zakresie działań prewencyjnych zapobiegających rozprzestrzenianiu się koronawirusa SARS-CoV-2" [11]. Dokument zawierał rekomendacje dla operatorów (właścicieli) obiektów infrastruktury krytycznej, wskazywał sposoby zapewnienia bezpiecznych warunków pracy, m. in. poprzez:

- przeprowadzenie wśród personelu akcji informacyjno-edukacyjnej w zakresie transmisji wirusa SARS-CoV-2, czasu inkubacji i występujących objawów, zasad postępowania ograniczających ryzyko zarażenia się wirusem, w tym zalecanych indywidualnych środków profilaktycznych,
- dokonanie zmian w organizacji pracy oraz zapewnienie dodatkowych środków bezpieczeństwa, tj. wprowadzenia pracy zdalnej, ograniczania kontaktów między pracownikami, zasad spożywania posiłków, ograniczenia

temperature measurements, more frequent disinfection and cleaning of surfaces,
– development of instructions on what to do if a worker develops symptoms suggesting the suspicion of being infected with SARS-CoV-2 virus on the premises of a given facility and beyond it, organisation of quarantine at the workplace.

The defined recommendations did not differ from the recommendations issued by the Chief Sanitary Inspectorate (GIS) for particular sectors and employers, yet due to its strategic importance critical infrastructure requires the adoption of additional solutions. Consequently, the document mentioned above contains provisions that provide a clear signal to critical infrastructure operators in Poland urging them to update their own protection plans. Pursuant to the regulation on critical infrastructure protection plans, the so-called POIK, these plans were developed by critical infrastructure operators, and after consultations they were approved by the director of the Government Security Centre (RCB) [12]. Critical infrastructure protection plans are updated as needed, at least once every two years. An undoubtedly real epidemiological hazard, which should be taken into account in the plans, resulted in the need to verify the operating procedures of the critical infrastructure operator planned for such a situation and having them adapted to conditions connected with COVID-19. The elements of the plan that needed to be reviewed were primarily measures to ensure the physical security of a specific facility and to limit access to such facility by third parties. However, the actions of the operators had to be much broader due to the risk of disease among the employees, and, above all, in the first place the necessity of protecting key personnel. Pursuant to regulation [12], plans of critical infrastructure protection contain operating variants, which might be undertaken in a situation of hazard or disruption to the functioning of critical infrastructure, ensuring the operating continuity of critical infrastructure and its reconstruction. The above procedures should be reviewed and updated to identify the criticality, uniqueness or specialisation of the role of the staff in order to minimise the necessity of keeping the employees at the work place. The guidelines/recommendations of RCB (guidelines) of March 2020 stated directly, that "in the scope oflaunching business continuity plansor other procedures aimed at regulating issues of the operator's functioning in case of unavailability of key personnel due to quarantine, illness or the need to care for children, it is necessary to monitor whether the above-mentioned plans and procedures are adequate to the current situation"[11] and should any disruptions occur to the provided services the critical infrastructure operator is obliged to take actions correcting the plan or the procedure.

In addition, the operators received a recommendation to prepare in advance for the "black scenario" and to devise appropriate policies to be followed should it become necessary to leave the facility by the staff working in it. The second variant recommended in the guidelines is mass remote work (i.e. leaving the so-called "skeleton crew" on site to enable safe operation of the facility and delegation of the remaining employees to carry out remote work [11]).

To ensure uninterrupted provision of services, those critical infrastructure operators that are able of doing so, were instructed

liczby punktów wejścia i wjazdu, obowiązkowej dezynfekcji rąk i pomiarów temperatury, częstszej dezynfekcji oraz sprzątania użytkowanej powierzchni,
– opracowanie instrukcji postępowania w przypadku wykrycia u pracownika objawów pozwalających na podejrzenie zarażenia wirusem SARS-CoV-2 na terenie obiektu oraz poza terenem obiektu, organizacji kwarantanny w miejscu pracy.

Zdefiniowane rekomendacje nie odbiegały od zaleceń wydawanych przez Główny Inspektorat Sanitarny (GIS) dla poszczególnych branż i pracodawców, jednak infrastruktura krytyczna – ze względu na strategiczne znaczenie – wymaga dodatkowych rozwiązań. W związku z powyższym wspomniany dokument zawiera zapisy, będące jasnym sygnałem dla operatorów IK w Polsce do dokonania aktualizacji planów ochrony dostosowanych swoich potrzeb. Zgodnie z rozporządzeniem w sprawie planów ochrony infrastruktury krytycznej operatorzy IK opracowali plany (POIK), które zostały zatwierdzone przez dyrektora Rządowego Centrum Bezpieczeństwa (RCB) [12]. POIK aktualizuje się według potrzeb, nie rzadziej niż raz na dwa lata. Niewątpliwie realne zagrożenie epidemiologiczne, które powinno być uwzględnione w planach, spowodowało potrzebę weryfikacji zaplanowanych na tą ewentualność procedur działania operatora IK do uwarunkowań związanych z COVID-19. Elementami planu, które wymagały tejże weryfikacji, były przede wszystkim działania na rzecz zapewnienia bezpieczeństwa fizycznego konkretnego obiektu oraz ograniczenia dostępu do takiego obiektu przez osoby trzecie. Działania operatorów – ze względu na ryzyko zachorowań wśród pracowników, a przede wszystkim konieczność ochrony kluczowego personelu – musiały mieć jednak znacznie szerszy zasięg. Zgodnie z rozporządzeniem [12] plany ochrony IK zawierają scenariusze działań w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej, zapewnienia ciągłości jej funkcjonowania oraz odtwarzania. Powyższe procedury powinny zostać zweryfikowane i zaktualizowane pod kątem określenia krytyczności, wyjątkowości lub specjalizacji roli pracowników w celu zmniejszenia potrzeby przebywania w miejscu pracy. Wytyczne/rekomendacje RCB z marca 2020 r. wskazały wprost, że „w zakresie uruchomienia planów ciągłości działania lub innych procedur, regulujących kwestie funkcjonowania operatora w przypadku niedostępności kluczowego personelu spowodowanej kwarantanną, chorobą lub koniecznością sprawowania opieki nad dziećmi, należy monitorować czy ww. plany i procedury są adekwatne do aktualnej sytuacji" [11], a w razie wystąpienia zakłóceń dla świadczonych usług operator IK ma obowiązek podjąć działania korygujące plan lub procedurę.

Ponadto operatorzy otrzymali rekomendację, aby z wyprzedzeniem przygotować się na „czarny scenariusz" i opracować zasady postępowania na wypadek konieczności całkowitego opuszczenia obiektu przez personel w nim zatrudniony. Drugi wariant rekomendowany w wytycznych, to masowa praca zdalna (tj. pozostawienia na terenie obiektu tzw. szkieletowej załogi, która umożliwi bezpieczne funkcjonowanie obiektu oraz oddelegowania pozostałych pracowników na pracę zdalną [11]).

Dla zapewnienia nieprzerwanego świadczenia usług operatorom IK, którzy mają taką możliwość, zalecono uruchomienie

to activate a parallel backup control station and to divide the dispatching services into two teams, while respecting the principle of no personal contacts between staff members of both posts.

The recommendations specified in the guidelines, being non-binding recommendations, required the introduction of additional solutions. It became necessary to introduce legal grounds for selected activities in order to ensure the continuity of operations of critical infrastructure operators during the SARS-COV-2 epidemic. The first formal decisions concerning combatting COVID-19, expressed by the Act of 2 March 2020 on specific solutions related to prevention, counteraction and suppression of COVID-19, other contagious diseases and crisis situations caused by them, the so-called Anti-Crisis Shield 1.0 [13], did not contain any provisions supporting critical infrastructure operators in the organisation of protective measures oriented at ensuring the continuity of critical infrastructure operation. It was only in the Act of 31 March 2020 amending the act on specific solutions related to prevention, counteraction and suppression of COVID-19, other contagious diseases and crisis situations caused by them, and some other acts, the so-called Anti-Crisis Shield 2.0 [14], that provisions have been adopted that allowed changing the system or the schedule of working time of the employees in the event of announcing an epidemic threat or the state of epidemic, article 15x of the COVID-19 Act [16]. This legislation was intended to ensure the resilience of critical infrastructure by securing the key resource, i.e. the employees, particularly during an epidemic. Moreover, the above-mentioned regulations allowed to secure not only the facilities included in the list of critical infrastructure, but also entities acting as subcontractors or suppliers, which are not part of the critical infrastructure, but are nevertheless key entities in maintaining the continuity of its activity.

Such entities obliged to protect (secure) key personnel, also include the following:

- enterprises running business activity consisting in assuring the functioning of transmission or distribution grids pursuant to Article 3 items 11a and 11b of the act of 10 April 1997 – The Energy Law (Polish Journal of Laws: Dz. U. z 2020 r. poz. 833, 843, 1086, 1378 i 1565);
- enterprises acting as subcontractor or supplier that assures the functioning of liquid fuel stations pursuant to Article 3 item 10h of the act dated 10 April 1997 – The Energy Law, and natural gas stations in understanding of Article 2 item 26 of the Act dated 11 January 2018 on electro mobility and alternative fuels (Polish Journal of Laws: Dz. U. z 2020 r. poz. 908 i 1086);
- enterprises acting as official sellers pursuant to Article 3 item 29 of the Act dated 10 April 1997 – The Energy Law;
- enterprises in the area or on the premises of a facility important for defence, economic interest of the state, public security and other important interests of the state as specified in Article 5 par. 1 and 2 of the Act dated 22 August 1997 on the protection of people and property comprised by listings specified in Article 5 par. 3 of the above mentioned act;
- entities carrying out the business of providing banking services pursuant to Article 5 of the Act dated 29 August

równolegle działającego zapasowego stanowiska kierowania oraz podział służb dyspozytorskich na dwa zespoły, przestrzegając zasady braku osobistych kontaktów między pracownikami obu stanowisk.

Określone w wytycznych rekomendacje, mające charakter niewiążących zaleceń, wymagały wprowadzenia dodatkowych rozwiązań. Konieczne okazało się stworzenie prawnych podstaw wybranych działań zapewniających ciągłość działania operatorów IK w sytuacji epidemii SARS-COV-2. Pierwsze ustalenia formalne dot. zwalczania COVID-19, wyrażone ustawą z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (tzw. Tarcza 1.0 [13]) nie zawierały zapisów umożliwiających wsparcie operatorów infrastruktury krytycznej w organizacji działań ochronnych na rzecz zapewnienia ciągłości funkcjonowania infrastruktury krytycznej. Dopiero w ustawie z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw (tzw. Tarcza 2.0 [14]) nastąpiło wprowadzenie przepisów, dających możliwość zmiany systemu lub rozkładu czasu pracy pracowników w przypadku ogłoszenia stanu zagrożenia epidemicznego albo stanu epidemii, art. 15x ustawy w sprawie COVID-19 [16]. Przepisy te miały na celu zapewnienie odporności infrastrukturze krytycznej poprzez zabezpieczenie kluczowego zasobu, jakim – zwłaszcza w sytuacji epidemii – są pracownicy. Co więcej, ww. przepisy pozwalały na zabezpieczenie nie tylko samych obiektów znajdujących się w wykazie infrastruktury krytycznej, ale także przedsiębiorstw będących podwykonawcą lub dostawcą, które nie wchodzą w skład infrastruktury krytycznej, ale są kluczowymi podmiotami dla zachowania ciągłości jej działania.

Do takich podmiotów, zobligowanych do ochrony (zabezpieczenia) kluczowego personelu zaliczono również:

- przedsiębiorstwa prowadzące działalność polegającą na zapewnieniu funkcjonowania sieci przesyłowych lub dystrybucyjnych w rozumieniu art. 3 pkt 11a i 11b ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2020 r. poz. 833, 843, 1086, 1378 i 1565);
- przedsiębiorstwa będące podwykonawcą lub dostawcą, zapewniające funkcjonowanie stacji paliw płynnych w rozumieniu art. 3 pkt 10h ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne oraz stacji gazu ziemnego w rozumieniu art. 2 pkt 26 ustawy z dnia 11 stycznia 2018 r. o elektromobilności i paliwach alternatywnych (Dz. U. z 2020 r. poz. 908 i 1086);
- przedsiębiorstwa pełniące funkcję sprzedawcy z urzędu w rozumieniu art. 3 pkt 29 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne;
- przedsiębiorstwa na obszarze lub na terenie obiektu ważnego dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa, o których mowa w art. 5 ust. 1 i 2 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, umieszczonych w wykazach, o których mowa w art. 5 ust. 3 tej ustawy;

1997 – the Banking Law (Polish Journal of Laws: Dz. U. z 2019 r. poz. 2357 oraz z 2020 r. poz. 284, 288, 321, 1086 i 1639;
– entities operating a category A extractive waste facility pursuant to Article 6 par. 1 item 1a a of the Act of 10 July 2008 on extractive waste (Polish Journal of Laws/ Dz. U. from 2017 item 1849 and from 2020 item 284), the operation or incorrect operation of which may cause a grave accident due to short-term or long-term loss of stability of such a facility, which may comprise all failures of mechanisms related to its structure or its incorrect usage that causes a considerable risk of death, significant health impairment or damage to the environment;
– enterprises operating in the agri-food sector related to the production or supply of foodstuffs.

It should be noted that some of these entities have already been identified during the development of CIP plans. In the part of the critical infrastructure protection plan related to dependencies of critical infrastructure on the remaining critical infrastructure systems and possibilities of disruptions to its functioning which may take place due to disruptions arising in the remaining systems of critical infrastructure, critical infrastructure operators identify entities and enterprises that are for example suppliers of raw materials or services necessary for appropriate functioning of a critical infrastructure facility.

Pursuant to provisions defined in the so-called Anti-Crisis Shield 2.0, employees working in critical infrastructure facilities and subsidiaries may be subject to barracks. In such a situation, the employer is obliged to provide accommodation and meals for the employee which would be sufficient for him/her to carry out the assigned duties. This involves the isolation of the worker in the workplace. The adopted regulations also enabled the above mentioned employers to:
– instruct the employees to work overtime within the scope and time indispensable to ensure the continuity of operation of the enterprise or station, as well as
– refuse granting vacation leave to the employee, including leave on demand, unpaid leave and other types of leave and to have such leave postponed, or
– recall an employee from vacation leave if such leave had already been granted to the employee [17–18].

The adoption of regulations interfering to such an extent with employees' rights resulted from the need to respond to a bigger risk that the number of employees in the above-mentioned entities would be reduced due to morbidity, and hence the risk of possible disruption of services (considered critical) could take place due to staff shortages.

A discussion regarding formal regulations or less formal guidelines relating to critical infrastructure operators would not have been complete without making reference to the recommendations developed by the Ministry of State Assets, the Ministry of Climate and the Government Security Centre on the basis of the guidelines of the Ministry of Development and the Chief Sanitary Inspectorate [18], which the Department of Security and Crisis Management of the Ministry of State Assets provided on 3 September 2020 to critical infrastructure operators of energy, energy

– przedsiębiorstwa prowadzące działalność polegającą na świadczeniu czynności bankowych w rozumieniu art. 5 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2019 r. poz. 2357 oraz z 2020 r. poz. 284, 288, 321, 1086 i 1639);
– przedsiębiorstwa prowadzące obiekt unieszkodliwiania odpadów wydobywczych kategorii A w rozumieniu art. 6 ust. 1 pkt 1 lit. a ustawy z dnia 10 lipca 2008 r. o odpadach wydobywczych (Dz. U. z 2017 r. poz. 1849 oraz z 2020 r. poz. 284), którego działanie lub niewłaściwe działanie może spowodować poważny wypadek, wynikający z krótkoterminowej lub długoterminowej utraty stateczności tego obiektu, obejmującej wszelkie awarie mechanizmów związanych z jego konstrukcją lub jego niewłaściwą eksploatacją, który skutkuje znacznym ryzykiem utraty życia, poważnego zagrożenia dla zdrowia ludzi lub środowiska;
– przedsiębiorstwa prowadzące działalność w sektorze rolno-spożywczym związane z wytwarzaniem lub dostarczaniem żywności.

Należy zaznaczyć, że część z tych podmiotów została zidentyfikowana już na etapie opracowywania planów ochrony infrastruktury krytycznej. W części planu ochrony IK dotyczących zależności infrastruktury krytycznej od jej pozostałych systemów oraz możliwości zakłócenia jej funkcjonowania w wyniku zakłóceń powstałych w pozostałych systemach infrastruktury krytycznej, operatorzy IK identyfikują podmioty i przedsiębiorstwa, które są np. dostawcami surowców, czy też usług zapewniających funkcjonowanie obiektu IK.

Na mocy przepisów zdefiniowanych w Tarczy 2.0 pracownicy obiektów IK i podmiotów zależnych mogą podlegać skoszarowaniu. Pracodawca obowiązany jest w takiej sytuacji zapewnić pracownikowi zakwaterowanie i wyżywienie niezbędne do realizacji przez pracownika jego obowiązków służbowych. Wiąże się to z izolacją pracownika w miejscu pracy. Wprowadzone przepisy stworzyły także wyżej wspomnianym pracodawcom możliwości:
– polecenia pracownikom świadczenia pracy w godzinach nadliczbowych w zakresie i wymiarze niezbędnym dla zapewnienia ciągłości funkcjonowania przedsiębiorstwa lub stacji, a także
– odmowy udzielenia pracownikowi urlopu wypoczynkowego, w tym urlopu na żądanie, urlopu bezpłatnego oraz innego urlopu, oraz przesuwania termin takiego urlopu lub
– odwołania pracownika z urlopu, jeżeli został on już pracownikowi udzielony [17–18].

Wprowadzenie tak daleko ingerujących w prawa pracownicze przepisów wynikało z potrzeby odpowiedzi na podwyższone ryzyko zmniejszonej liczby pracowników wspomnianych wcześniej przedsiębiorstw w związku z zachorowaniami, a tym samym ryzykiem możliwych zakłóceń w realizacji usług (uznanych za krytyczne) ze względu na niedobory kadrowe.

Dyskusja dotycząca formalnych przepisów lub mniej formalnych wytycznych odnosząca się do operatorów infrastruktury krytycznej byłaby niepełna bez informacji o zaleceniach opracowanych przez Ministerstwo Aktywów Państwowych, Ministerstwo

raw materials and fuel supply system and to distribution system operators and the transmission system operators.

The above-mentioned recommendations covered 4 main themes [18]:

1. Further increase in safety of employees of authorities/institutions, employees of companies that serve authorities/ institutions and customers (guidelines for employers; guidelines for employees; guidelines for visitors; rules for the reception of visitors; rules for handling various issues in seats of state authorities and institutions).
2. Minimising the risk of infection of staff working for authorities/institutions, employees of enterprises that serve authorities/institutions and customers.
3. Limiting the number of contacts on the premises of authorities/institutions in a given time period as a safeguard against possible infection.
4. Complex counter-epidemic actions appropriately adjusted to the state of the epidemic.

The recommendations specified above allowed defining preventive procedures: suspected SARS-CoV-2 infection of a worker/ maintenance worker, as well as the procedures to be followed in case of suspected SARS-CoV-2 infection of worker/customer. In addition, they detailed rules for ensuring safety inside facilities, especially in industrial plants, fuel stations, as well as food courts and foodstuff sale areas situated in them. The recommendations have also determined the procedure of "quick flight" applicable to:

– key staff members of sectors supervised by the Minister of Climate who have been considered to be of key importance, and
– employees of key operators supplying energy, energy raw materials and fuels, as well the distribution system operators and the transmission system operator.

The situation caused by COVID-19 verified the preparation of critical infrastructure operators to maintain business continuity. They forced the operators to activate the existing, implemented and maintained solutions adopted within the so-called business continuity management system, i.e. plans for maintaining operating continuity and emergency plans. In their planning and pre-implementation works, critical infrastructure operators have identified key personnel and protective measures meant to assure its availability in line with the adopted method of organisation and implementation of the operating continuity system. In the cited plans, they also defined on an on-going basis the minimum (indispensable) resources necessary to assure the operating continuity of critical processes of the organisation. Those operators who had an implemented operating continuity system verified with respect to its functionality were able to cope much better in the face of COVID-19 [19].

Klimatu oraz Rządowe Centrum Bezpieczeństwa na podstawie wytycznych Ministerstwa Rozwoju oraz Głównego Inspektoratu Sanitarnego [18]. Wymienione wytyczne Departament Bezpieczeństwa i Zarządzania Kryzysowego Ministerstwa Aktywów Państwowych przekazał w dniu 3 września 2020 r. operatorom infrastruktury krytycznej systemu zaopatrzenia w energię surowce energetyczne i paliwa, a także operatorom systemów dystrybucyjnych oraz operatorowi systemu przesyłowego.

Przedmiotowe zalecenia obejmowały cztery główne obszary tematyczne [18]:

1. Dodatkowe zwiększenie bezpieczeństwa pracowników urzędu/instytucji, pracowników firm obsługujących urząd/instytucję oraz interesantów (wytyczne dla pracodawców, wytyczne dla pracowników, wytyczne dla gości, zasady przyjmowania gości, zasady załatwiania spraw w urzędach i instytucjach państwowych).
2. Minimalizowanie ryzyka zakażenia pracowników urzędu/ instytucji, pracowników firm obsługujących urząd/instytucję oraz interesantów.
3. Ograniczenie liczby kontaktów na terenie urzędu/instytucji w danym przedziale czasowym, w ramach zabezpieczenia przed możliwym zakażeniem.
4. Kompleksowe działanie przeciwepidemiczne dostosowane do etapu zaawansowania stanu epidemii.

Nadmienione zalecenia zdefiniowały procedury zapobiegawcze zarówno podejrzenie zakażenia SARS-CoV-2 u pracownika/ obsługi, jak również procedury postępowania w przypadku podejrzenia zakażenia SARS-CoV-2 u pracownika/interesanta. Dodatkowo szczegółowo precyzowały zasady zapewnienia bezpieczeństwa w obiektach, zwłaszcza w zakładach przemysłowych, stacjach paliw oraz zlokalizowanych w nich strefach gastronomicznych i strefach sprzedaży żywności. Zalecenia określiły również procedurę „szybkiej ścieżki" odnoszącą się do:

– kluczowych pracowników sektorów nadzorowanych przez Ministra Klimatu, które zostały uznane za kluczowe oraz
– pracowników kluczowych operatorów systemu zaopatrzenia w energię, surowce energetyczne i paliwa, a także operatorów systemów dystrybucyjnych i operatora systemu przesyłowego.

Uwarunkowania COVID-19 zweryfikowały przygotowania operatorów infrastruktury krytycznej do utrzymania ciągłości działania. Wymusiły na operatorach aktywację posiadanych, wdrożonych i utrzymywanych rozwiązań przyjętych w ramach tzw. systemu zarządzania ciągłością działania (tj. planów utrzymania ciągłości działania oraz planów awaryjnych). W ramach prac planistycznych, przedwdrożeniowych, zgodnie z przyjętą metodyką organizacji i wdrażania systemu zarządzania ciągłości działania, operatorzy infrastruktury krytycznej zdefiniowali personel kluczowy oraz działania ochronne na rzecz zapewnienia jego dostępności. W przywoływanych planach każdorazowo określali również minimalne zasoby niezbędne do utrzymania ciągłości działania krytycznych procesów organizacji. Operatorzy, którzy posiadali wdrożony i zweryfikowany pod względem funkcjonalnym system zarządzania ciągłości działania, znacznie łatwiej odnaleźli się w rzeczywistości COVID-19 [19].

Summary / Conclusions

The reality of COVID-19 has exposed the inadequacy of laws and procedures in the scope of non-standard behaviour of the employers towards the employees of elements considered as critical infrastructure of the state. The epidemic, included in the catalogue of 20 threats considered in the National Crisis Management Plan 2020, has clearly been underestimated, at least in terms of its possible effects on the society. Concurrently, the nature and the spreading rate of the SARS-CoV-2 virus have proven individualised to such an extent that they have become a global problem, a challenge, which was handled by individual countries in a more or less restrictive manner. This situation may be perceived in terms of a worldwide crisis which has not yet ended and the overcoming of which requires efforts, discipline and solutions at the national level. The first legal decisions in Poland related to specific solutions associated with prevention, counteracting and eradication of COVID-19, other contagious diseases and the ensuing crisis situations were announced on 2 March 2020, but they did not comprise solutions supportive to strengthening the protection of critical infrastructure yet. The first guidelines in this respect were provided to the critical infrastructure operators by the Government Security Centre on 16 March 2020. The guidelines specified recommendations for the operators of critical infrastructure referring to the conditions of the spread of the virus, adopting changes to work organisation and adoption of additional security means, or the development of instructions on what to do if a worker develops symptoms suggesting the infection with SARS-CoV-2 on the facility premises and off-site, organisation of quarantine in the work place etc. The update of the COVID-19 Act, the so-called Anti-Crisis Shield 2.0 [14], announced on 31 March 2020, introduced regulations that permitted the adoption of changes to the employee work system or the working time schedule of employees to be changed in the event of announcing an epidemic threat or a state of epidemic, article 15x of the COVID-19 Act [15]. Those regulations have become a tool for enhancing the resilience of critical infrastructure thanks to the possibility of securing the key resource, i.e. employees, thus ensuring the uninterrupted functioning of critical infrastructure, as well as staff of enterprises acting as a subcontractor or supplier that may not be a part of critical infrastructure, nevertheless they may be key players in maintaining business continuity of critical infrastructure operations. In terms of legal measures taken to minimise the risk of threats to critical infrastructure, *de lege ferenda* conclusions have also been defined in the literature on the subject. They refer to [15, p. 7]:

- the need to consider adding entities operating under systems which have been granted special authorisations pursuant to Article 15x of the COVID-19 Act to the inventory of critical infrastructure,
- taking into consideration the need of devising regulations to be adopted as extraordinary ones to the formula of the so-called dormant regulations, which are to be automatically activated during similar crises in the future,
- the possibility of preparing and delegating some of the staff (as the so-called substitute staff) to execute

Podsumowanie / Wnioski

Rzeczywistość COVID-19 obnażyła niewystarczający charakter przepisów i procedur w zakresie umożliwiających ponadstandardowe zachowania pracodawców wobec pracowników – elementów uznanych za infrastrukturę krytyczną państwa. Epidemia, mieszcząca się w katalogu 20 zagrożeń rozpatrywanych w Krajowym Planie Zarządzania Kryzysowego 2020, niewątpliwie nie została doszacowana – przynajmniej w zakresie możliwych skutków oddziaływania na społeczeństwo. Równocześnie charakterystyka i tempo rozprzestrzeniania się wirusa SARS-CoV-2 okazały się na tyle zindywidualizowane, że stały się problemem ogólnoświatowym, wyzwaniem do którego poszczególne państwa podchodziły w bardziej lub mniej restrykcyjny sposób. Zaistniała sytuacja może być określana w kategoriach ogólnoświatowego kryzysu, który wciąż trwa i do pokonania którego niezbędne są wysiłki, dyscyplina i rozwiązania na poziomie poszczególnych państw. Pierwsze rozwiązania prawne w Polsce, dotyczące szczególnych narzędzi związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, zostały ogłoszone w dniu 2 marca 2020 r., przy czym nie zawierały one jeszcze rozwiązań umożliwiających wzmocnienie ochrony infrastruktury krytycznej. Pierwsze wytyczne w tym zakresie zostały przekazane operatorom infrastruktury krytycznej przez Rządowe Centrum Bezpieczeństwa w dniu 16 marca 2020 r. Zawierały rekomendacje dla operatorów infrastruktury krytycznej odnoszące się do uwarunkowań rozprzestrzeniania się wirusa, dokonywania zmian w organizacji pracy i wprowadzania dodatkowych środków bezpieczeństwa, czy też opracowania instrukcji postępowania w przypadku wykrycia u pracownika objawów pozwalających na podejrzenie zarażenia wirusem SARS-CoV-2 na terenie obiektu oraz poza terenem obiektu, organizacji kwarantanny w miejscu pracy itd. Ogłoszona w dniu 31 marca 2020 r. aktualizacja ustawy [14] tzw. Tarcza 2.0 wprowadziła przepisy dające możliwość zmiany systemu lub rozkładu czasu pracy pracowników w przypadku ogłoszenia stanu zagrożenia epidemicznego albo stanu epidemii, art. 15x tej ustawy [15]. Rzeczone przepisy stały się narzędziem do wzmacniania odporności infrastruktury krytycznej dzięki możliwości zabezpieczenia kluczowego zasobu – pracowników zapewniających nieprzerwane funkcjonowanie infrastruktury krytycznej oraz personelu przedsiębiorstw będących podwykonawcą lub dostawcą, którzy nie wchodzą wprawdzie w skład infrastruktury krytycznej, ale są kluczowymi podmiotami dla zachowania ciągłości jej działania. W aspekcie działań prawnych podejmowanych na rzecz minimalizowania ryzyka występowania zagrożeń dla infrastruktury krytycznej, w literaturze przedmiotu zdefiniowano także wnioski o charakterze *de lege ferenda*. Odnoszą się one do [15, s. 7]:

- potrzeby rozważenia dodania podmiotów funkcjonujących w ramach systemów, które otrzymały specjalne uprawnienia na mocy art. 15x ustawy w sprawie COVID-19, do wykazu infrastruktury krytycznej,
- rozważenia potrzeby przygotowania przepisów wprowadzonych jako nadzwyczajne do formuły tzw. przepisów uśpionych, aktywowanych automatycznie w czasie kolejnych analogicznych kryzysów przyszłości,

activities meant to ensure the operating continuity of critical infrastructure in a situation with critical shortage of key employees in the organisation.

When defining the above conclusions, it should be borne in mind that experience gained by critical infrastructure operators related to the functioning in COVID-19 pandemic is not only a fact of the past, but still continues to be gained. In the period following the pandemic, the Government Security Centre should organise a nationwide protection forum for critical infrastructure dedicated to an exchange of experience between forum participants, while the presented practices and solutions should be formalised as good practices and recommendations and then propagated among stakeholders of the critical infrastructure protection system in Poland.

– możliwości przygotowywania i oddelegowywania części personelu (jako tzw. personelu zastępczego) do realizacji działań zapewniających ciągłość działania infrastruktury krytycznej w sytuacji niebezpiecznego w skutkach niedoboru kluczowego personelu.

Definiując powyższe wnioski, należy pamiętać, że zdobywanie przez operatorów infrastruktury krytycznej doświadczenia związanego z funkcjonowaniem w warunkach COVID-19 nie jest tylko faktem z przeszłości, ale odbywa się nadal. W warunkach popandemicznych zadaniem Rządowego Centrum Bezpieczeństwa powinna być organizacja ogólnokrajowego forum ochrony infrastruktury krytycznej poświęconego wymianie doświadczeń pomiędzy uczestnikami wydarzenia, zaś zaprezentowane działania i rozwiązania należy sformalizować w formie dobrych praktyk i rekomendacji oraz rozpowszechnić wśród interesariuszy systemu ochrony infrastruktury krytycznej w Polsce.

Literature / Literatura

[1] Wróbel R., Gromek P., *Ochrona obiektów kluczowych. Zarządzanie kryzysowe, ryzykiem i ciągłością działania*, Wyd. SGSP, Warszawa 2018.

[2] Wróbel R., Gromek P., *Ochrona obiektów kluczowych. Perspektywa bezpieczeństwa powszechnego*, Wyd. SGSP, Warszawa 2017.

[3] Soloch P., *NATO a ochrona infrastruktury krytycznej*, http://www.bbn.gov.pl/dokumenty/nato_a_ochrona_infrastruktury_krytycznej.pdf [dostęp: 14.05.2021].

[4] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2021, poz. 159).

[5] Rządowe Centrum Bezpieczeństwa, Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik nr 2 – Kryteria, Warszawa 2020.

[6] Wróbel R., *Przygotowanie podmiotów ochrony infrastruktury krytycznej w Polsce*, Wyd. SGSP, Warszawa 2016.

[7] Rządowe Centrum Bezpieczeństwa, Krajowy Plan Zarządzania kryzysowego. Aktualizacja 2020. Część A, Warszawa 2020.

[8] Główny Inspektorat Weterynarii, Polski Plan Pandemiczny 2009, Warszawa 2009.

[9] Centrum Polityk Publicznych, Zarządzanie zasobami ludzkimi w systemie ochrony zdrowia w czasach pandemii, Kraków 2020, https://politykipubliczne.pl/wp-content/uploads/2020/10/09-Ochrona-zdrowia_16.09.2020-last.pdf [dostęp: 14.05.2021].

[10] Kulik I., *System zarządzania kryzysowego w ochronie infrastruktury krytycznej województwa*, praca doktorska, AON, Warszawa 2016.

[11] Rządowe Centrum Bezpieczeństwa, *Wytyczne dla operatorów infrastruktury krytycznej w zakresie działań prewencyjnych zapobiegających rozprzestrzenianiu się koronawirusa SARS-CoV-2*, Warszawa 2020, s. 7–8, https://www.gov.pl/web/aktywa-panstwowe/zalecenia-zwiazane-z-epidemia-sars-cov-2 [dostęp: 14.05.2021].

[12] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz. U. 2010 Nr 83, poz. 542).

[13] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. 2020, poz. 374).

[14] Ustawa z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw (Dz. U. 2020, poz. 568).

[15] Mikusek P., *Ochrona ciągłości funkcjonowania infrastruktury krytycznej w obliczu kryzysu epidemicznego COVID-19*, Instytut Mikołaja Siennickiego, Warszawa 2020, https://instytut-sienickiego.pl/wp-content/uploads/2021/04/2020.05.31_Infrastruktura_krytyczna_w_dobie_COVID-19.docx.pdf [dostęp: 14.05.2021].

[16] Kicińska A., *Skoszarowanie pracowników. Poradnik dla pracodawców branży ciepłowniczej*, Sienkiewicz i Zamroch Radcowie Prawni Spółka Partnerska, Warszawa 2020, https://prawodlapracodawcy.pl/wp-content/uploads/2020/11/Skoszarowanie-pracownikow-poradnik.pdf [dostęp: 14.05.2021].

[17] https://prawodlapracodawcy.pl/skoszarowanie-pracownikow-w-czasie-epidemii/ [dostęp: 14.05.2021].

[18] Zalecenia Ministra Aktywów Państwowych, Ministra Klimatu oraz Dyrektora Rządowego Centrum Bezpieczeństwa dla urzędów i instytucji państwowych, jednostek podległych i nadzorowanych przez Ministra Aktywów Państwowych i Ministra Klimatu oraz Operatorów Infrastruktury

Krytycznej systemu zaopatrzenia w energię, surowce energetyczne i paliwa, a także Operatorów Systemów Dystrybucyjnych i Operatora Systemu Przesyłowego, Warszawa, wrzesień 2020, https://www.gov.pl/web/aktywa-panstwowe/zalecenia-zwiazane-z-epidemia-sars-cov-2 [dostęp: 14.05.2021].

[19] Gałaj-Emiliańczyk K., *Ciągłość działania przedsiębiorstw w dobie pandemii*, https://www.bureauveritas.pl/magazine/ciaglosc-dzialania-przedsiebiorstw-w-dobie-pandemii [dostęp: 14.05.2021].

RAFAŁ WRÓBEL, PH.D. – a graduate of the Main School of Fire Service and the National Defense University, an officer of the State Fire Service, head of the Department of Decision Process Engineering of the Main School of Fire Service (SGSP), in the past the Dean of the Department of Security and Civil Protection at SGSP. Author and co-author of four monographs and several dozen scientific articles, author and executor of national and foreign projects.

ILONA WRÓBEL, PH.D. – in the past, an academic teacher at the Military Art Academy, a doctor of security sciences. In 2016, she completed doctoral studies at the National Security Department of the National Defense University in Warsaw. Coordinator of a project "Popularization and dissemination of knowledge about state defense and the activities of the Armed Forces of the Republic of Poland among students from Masovian, Świętokrzyskie and Lubelskie junior high and high schools" and a lecturer as part of a training "Education for security" and "Preparation for a terrorist attack" under a project co-financed by the European Union PROJECT No. PO KL. 09.04.00-14-110/09 "Education for safety and effective teacher-student communication". She conducted lectures and workshops in the field of security and defense, including for the Ministry of the Environment, the Ministry of Economy, the Internal Security Agency, the National Prosecutor's Office, MZA Sp. z o.o. in Warsaw, PKP PLK and other entities. She gained practical experience in the field of crisis management and defense at the province level. In her professional work, she develops the issues of civil-military cooperation and crisis management. Author of numerous articles on national security.

DR RAFAŁ WRÓBEL – absolwent Szkoły Głównej Służby Pożarniczej i Akademii Obrony Narodowej, funkcjonariusz Państwowej Straży Pożarnej, kierownik Zakładu Inżynierii Procesów Decyzyjnych Szkoły Głównej Służby Pożarniczej, w przeszłości Dziekan Wydziału Bezpieczeństwa i Ochrony Ludności w SGSP. Autor i współautor czterech monografii i kilkudziesięciu artykułów naukowych, autor i wykonawca krajowych i zagranicznych projektów.

DR ILONA WRÓBEL – w przeszłości nauczyciel akademicki Akademii Sztuki Wojennej, doktor nauk o bezpieczeństwie. W 2016 r. ukończyła studia doktoranckie na Wydziale Bezpieczeństwa Narodowego Akademii Obrony Narodowej w Warszawie. Koordynator projektu „Popularyzowanie i upowszechnianie wiedzy na temat obronności państwa i działalności Sił Zbrojnych RP wśród uczniów mazowieckich, świętokrzyskich i lubelskich szkół gimnazjalnych i ponadgimnazjalnych" oraz wykładowca w ramach szkolenia „Edukacja na rzecz bezpieczeństwa" oraz „Przygotowanie na atak terrorystyczny" w ramach projektu współfinansowanego przez Unię Europejską PROJEKT nr PO KL. 09.04.00-14-110/09 „Edukacja na rzecz bezpieczeństwa i skuteczna komunikacja nauczyciel – uczeń". Prowadziła wykłady i warsztaty z zakresu bezpieczeństwa i obronności m.in. dla Ministerstwa Środowiska, Ministerstwa Gospodarki, Agencji Bezpieczeństwa Wewnętrznego, Prokuratury Krajowej, MZA Sp. z o.o. w Warszawie, PKP PLK i innych podmiotów. Doświadczenie praktyczne zdobywała w obszarze zarządzania kryzysowego i obronności na poziomie powiatu. W pracy zawodowej rozwija problematykę współpracy cywilno-wojskowej oraz zarządzania kryzysowego. Autorka licznych artykułów z zakresu bezpieczeństwa narodowego.