Małgorzata Czuryk*

Cybersecurity as a premise to introduce a state of exception

Abstract

A significant threat to the security of a State, and its citizens, which cannot be mitigated with the use of standard procedures, i.a., without restricting human and civil rights and freedoms, can result in the establishment of a state of exception (martial law, state of emergency, state of natural disaster). A cybersecurity threat is considered to be one of the premises for introducing such a state. Due to cybersecurity issues, the President of the Republic of Poland (martial law, state of emergency) and the Council of Ministers (state of natural disaster) may introduce a state of exception. Threats in cyberspace might prove significant enough from the point of view of the functioning of the State, its authorities, and the public, to substantiate the announcement of a state of exception.

Key words: cybersecurity, martial law, state of emergency, state of natural disaster

* Małgorzata Czuryk, Ph.D. hab., Professor at UWM, the Faculty of Law and Administration, the University of Warmia and Mazury in Olsztyn, e-mail: malgorzata.czuryk@uwm.edu.pl, ORCID: 0000-0003-0362-3791.

In the event of an external threat to the State, including as a result of terrorist acts or activities in cyberspace, an armed attack on the territory of the Republic of Poland, or an obligation to ensure joint defence against aggression under international agreements, at the request of the Council of Ministers, the President of the Republic of Poland may introduce martial law across the entire territory of the country, or its part[1]. External threats to the State can also be caused by incidents taking place in cyberspace. Terrorist acts might also be perpetrated in cyberspace, and consequently cyberterrorism can become a circumstance substantiating the announcement of martial law.

By analogy, a cybersecurity threat is one of the potential conditions for the introduction of a state of emergency. Therefore, in the event of a substantial threat to the constitutional State system, the security of citizens or public order, including threats arising from terrorist acts or activities in cyberspace, which cannot be eliminated with the use of standards constitutional procedures, the Council of Ministers may adopt a resolution on submitting a request to the President of the Republic of Poland to introduce a state of emergency[2]. A substantial threat to the constitutional State system, the security of citizens or public order, justifying a state of emergency, might arise from the need to protect cybersecurity.

As regards the state of a natural disaster, it is possible that events in cyberspace and terrorist acts might contribute to the occurrence of a natural catastrophe or a technical failure (being premises to announce such a state)[3]. As per Article 2 of the Act on the State of a Natural Disaster (ASND), the state of a natural disaster may be introduced to prevent the consequences of natural catastrophes or technical failures with natural-disaster characteristics, and to eliminate such consequences. The legislators have defined the notions of a natural disaster, a natural catastrophe, and technical failure. In accordance

1 Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, t.j., Dz.U. 2017, poz. 1932, art. 2, ust. 1 („the MLA", or „the Martial Law Act"). For more details, refer to M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, nr 3.

2 Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, t.j., Dz.U. 2017, poz. 1928, art. 2, ust. 1. For more details, refer to M. Karpiuk, *Normatywne uwarunkowania stanu wojennego i wyjątkowego*, „Studia Prawnicze i Administracyjne" 2015, nr 3, s. 6.

3 Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, t.j., Dz.U. 2017, poz. 1897, art. 3, ust. 2 („ASND" – or The Act on the State of Natural Disaster). See M. Czuryk, *Activities of the Local Government During a State of Natural Disaster*, „Studia Iuridica Lublinensia" 2021, nr 4, s. 115.

with Article 3 (1) (1) of the ASND, a natural disaster is a natural catastrophe or a technical failure whose consequences affect the lives and health of a large population, property of a significant size, or the environment across a vast area, where aid and protection can be effective only by applying extraordinary measures as part of collaboration between various authorities and institutions, as well as specialised services and units under a single management. As per Article 3 (1) (2) of the ASND, a natural catastrophe means an event related to natural phenomena, in particular thunderstorms, seismic tremors, strong winds, intense rainfall or snowfall, long-term extreme temperatures, landslides, fire, draught, flood, ice-related phenomena on rivers, seas, lakes, and other water reservoirs, the widespread occurrence of pests, plant or animal diseases, or infectious diseases in humans, or the impact of other elements. In turn, pursuant to Article 3 (1) (3) of the ASND, a technical failure is sudden and unexpected damage to, or destruction of, a building, a technical device, or a system of technical devices resulting, in a disruption to their operations, or the loss of their properties[4].

A given state of exception may be introduced subject to meeting specified constitutional conditions. In the event of a considerable threat, if standard constitutional measures are inadequate, an applicable state of exception – martial law, state of emergency, state of natural disaster – may be introduced. They may only be brought in on statutory grounds, by way of a regulation which is subject to the obligation of an accompanying public announcement. Any actions to be undertaken as a result of one of the states of exception must correspond to the level of threat, and should be aimed at restoring the normal functioning of the State as fast as possible[5]. States of exception require the occurrence of a considerable risk to the State and its citizens. This includes extraordinary threats which exceed normal levels[6]. The Polish Constitution does not refer to cyberspace as a place in which a threat requiring the introduction of a state of exception occurs, but this condition is specified in Acts referring to individual states of exception.

4 For more details, refer to M. Czuryk, *Zadania organów jednostek samorządu terytorialnego w stanie klęski żywiołowej*, „Zeszyty Naukowe AON" 2009, nr 3, s. 405–407; M. Karpiuk, *Kształtowanie się instytucji stanów nadzwyczajnych w Polsce*, Warszawa 2013, s. 145–147.

5 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483, art. 228 („the Polish Constitution").

6 P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku*, Warszawa 2008, s. 428.

A state of exception is not an implied or discretionary state which can be identified on the basis of criteria devised by an entity assessing a given situation, but it is a normative state, arising from the application of specific legal solutions[7]. The introduction of a state of exception is not a decision made at the discretion of the responsible State authorities, but it is a consequence of the occurrence of strictly defined circumstances. A state of exception may only be introduced on statutory grounds, and a regulation to that effect constitutes an appropriate form of this action. In addition to its mandatory publication in the Journal of Laws, similarly to other legal acts of this kind, such a regulation is subject to an accompanying public announcement, in a form which is easily accessible to all citizens. There are multiple forms of announcement. These are not listed in the Constitution, and depend on local conditions and standard procedures. The most frequently used forms include public notices, posters, as well as radio and television communications. Introducing a state of exception affects the principles by which public authorities operate, and the range of freedoms and rights vested in individuals. These are not issues to be decided by the authorities, as they have been defined in the Constitution and in the acts governing individual states of exception. The authorities are not empowered to freely define the consequences of introducing the said states, as they have been provided for in the Acts. The rules and procedures for compensating for property loss arising from the introduced restrictions may only be regulated by the applicable acts[8].

A state of exception may be introduced in line with prescriptive criteria, which include, i.a., a threat caused by activities in cyberspace (martial law, state of emergency), or an incident in cyberspace (state of natural disaster). These criteria should not be interpreted freely. A cybersecurity breach might constitute a condition for introducing a given state of emergency, but only if the resulting threat is significant, and cyberspace cannot be protected otherwise to ensure the security of the State and its institutions.

Consequently, a state of exception may be introduced due to activities in cyberspace, understood as a sphere for the processing and exchange of information, created by information and communication systems (ICT systems). An ICT system, as a determinant of cyberspace, is a set of interfacing IT hardware and software, providing the facility to process, store, send, and

7 Postanowienie SN z dnia 28 lipca 2020 r., I NSW 4482/20, LEX nr 3035359.

8 W. Skrzydło, *Komentarz do art. 228 Konstytucji RP* [w:] idem, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2013, LEX/el.

receive data via ICT networks, with the use of an end-device suitable for a given network type[9].

The objective of each state of exception is to counteract threats and rescue the common good[10]. Common good constitutes the foundation of public order and the system of a democratic State of law, so the ultimate goal which the public authorities strive to fulfil. Common good is not a one-dimensional category, which makes it difficult to define, although it does not mean that public authorities may waive their responsibility for the fulfilment of this objective[11]. Cybersecurity is also a common good which must be protected by law, also by way of introducing one of the states of exception, thus it acquires a special significance, as it is vital from the perspective of the normal functioning of the State and the information society.

The basic requirement placed on public authorities in respect of a state of exception is its proportionality to the level of the threat. Therefore, such an authority cannot undertake measures which are burdensome to the public, but not unsubstitutable if more moderate actions can be pursued to reach the same objective. A public authority responsible for taking the appropriate actions is every time responsible for assessing which measure should be applied[12].

Cybersecurity is one of the domains of security[13] which is currently gaining a special significance as the information society is developing. Cybersecurity has been defined under legal regulations, and it means the ability of information systems to resist actions which compromise the confidentiality, integrity, availability, and authenticity of processed data, or the related services provided by those information systems[14]. The security of network

9 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j., Dz.U. 2021, poz. 670, art. 3, pkt 3.

10 B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, s. 967.

11 M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3, s. 15.

12 M. Czuryk, *Podstawy prawne bezpieczeństwa narodowego w stanie kryzysu i wojny*, „Roczniki Nauk Społecznych" 2013, nr 3, s. 70.

13 Security is one of the primary needs of humans which should be satisfied both by public and private entities, and by the persons concerned themselves, insofar as they are able to meet these needs, M. Karpiuk, *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, nr 2, s. 67.

14 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j., Dz.U. 2020, poz. 1369, z późn. zm., art. 2, pkt 4 (the NCSA – the National Cybersecurity System Act). For detailed information on cybersecurity, refer to: K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The Legal Status of Public Entities in the Field of Cybersecurity in*

and information systems means the ability of network and information systems to resist any action which compromises the availability, authenticity, integrity, or confidentiality of stored or transmitted or processed data, or the related services provided by, or accessible via, those network and information systems[15]. The requirement to ensure the protection of information systems might impose the need to introduce an applicable state of exception in order to protect the interests which are essential from the point of view of the State authorities and their exercising of powers.

As per Article 2 (14) of the National Cybersecurity System Act, an information system is an ICT system, together with the electronic data processed in such a structure. In turn, under Article 4 (1) of the NIS Directive, a network and information system means 1) an electronic communications network (including transmission systems, whether or not based on a permanent infrastructure or a centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical, or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed[16]; 2) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform the automatic processing of digital data; or 3) digital data stored, processed, retrieved, or transmitted by elements covered under the above points for the purposes of their operation, use, protection, and maintenance.

The security of networks and information systems operated by digital service providers is an important aspect of the context of cybersecurity.

Poland, Maribor 2021; I. Hoffman, K.B. Cseh, *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, „Cybersecurity and Law" 2020, nr 2; I. Hoffman, *Cybersecurity and public administration in the time of corona(virus) – in the light of the recent Hungarian challenges*, „Cybersecurity and Law" 2021, nr 1.

15 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE 2016, L 194, art. 4, pkt 1–2 („the NIS Directive").

16 Dyrektywa Parlamentu Europejskiego i Rady (UE) z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej, ibidem 2018, L 321, art. 2, pkt 1, s. 36.

Given the above sphere, EU Member States are obligated to ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of providing services within the Union. Having regard to the state of the art, these measures must ensure a level of security of network and information systems appropriate to the risk posed, and take into account the following elements: 1) the security of the systems and facilities; 2) incident handling; 3) business continuity management; 4) monitoring, auditing, and testing; and 5) compliance with international standards. These aspects of cybersecurity were addressed in Article 16 (1) of the NIS Directive. The security of systems and facilities means the security of network and information systems and of their physical environment, and must include the following elements: 1) the systematic management of network and information systems, which means a mapping of information systems, and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, security of operations, security architecture, secure data and system life cycle management, and, where applicable, encryption and its management; 2) physical and environmental security, which means the availability of a set of measures to protect the security from damage of digital service providers' network and information systems using an all-hazards risk-based approach, addressing, for instance, system failure, human error, malicious action, or natural phenomena; 3) the security of supplies, which means the establishment and maintenance of the appropriate policies in order to ensure the accessibility, and, where applicable, the traceability of critical supplies used in the provision of the services; 4) access controls to network and information systems, which means the availability of a set of measures to ensure that the physical and logical access to network and information systems, including the administrative security of network and information systems, is authorised and restricted, based on business and security requirements[17].

17 Rozporządzenie wykonawcze Komisji UE 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ, ibidem, L 26, art. 2, ust. 1, s. 48.

Bibliography

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009.
Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021.
Czuryk M., *Activities of the Local Government During a State of Natural Disaster*, „Studia Iuridica Lublinensia" 2021, nr 4.
Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3.
Czuryk M., *Podstawy prawne bezpieczeństwa narodowego w stanie kryzysu i wojny*, „Roczniki Nauk Społecznych" 2013, nr 3.
Czuryk M., *Zadania organów jednostek samorządu terytorialnego w stanie klęski żywiołowej*, „Zeszyty Naukowe AON" 2009, nr 3.
Hoffman I., *Cybersecurity and public administration in the time of corona(virus) – in the light of the recent Hungarian challenges*, „Cybersecurity and Law" 2021, nr 1.
Hoffman I., Cseh K.B., *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, „Cybersecurity and Law" 2020, nr 2.
Karpiuk M., *Kształtowanie się instytucji stanów nadzwyczajnych w Polsce*, Warszawa 2013.
Karpiuk M., *Normatywne uwarunkowania stanu wojennego i wyjątkowego*, „Studia Prawnicze i Administracyjne" 2015, nr 3.
Karpiuk M., *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, nr 3.
Karpiuk M., *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, nr 2.
Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2013.
Winczorek P., *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku*, Warszawa 2008.

Cyberbezpieczeństwo jako przesłanka wprowadzenia stanu nadzwyczajnego

Streszczenie

Szczególne zagrożenie bezpieczeństwa państwa i jego obywateli, którego nie da się zniwelować zwykłymi środkami, w tym m.in. bez ograniczania wolności i praw człowieka i obywatela – mogą prowadzić do ogłoszenia stanu nadzwyczajnego (stanu wojennego, stanu wyjątkowego, stanu klęski żywiołowej). Jedną z przesłanek uzasadniających wprowadzenie takiego stanu jest cyberbezpieczeństwo. Ze względu na cyberbezpieczeństwo Prezydent RP (stan wojenny, stan wyjątkowy) oraz Rada Ministrów (stan klęski żywiołowej) może wprowadzić stan nadzwyczajny. Zagrożenia występujące w cyberprzestrzeni będą zatem na tyle ważne z punktu widzenia funkcjonowania państwa i jego organów, a także społeczeństwa, że dopuszcza się ze względu na nie wprowadzenie stanu nadzwyczajnego.

Słowa kluczowe: cyberbezpieczeństwo, stan wojenny, stan wyjątkowy, stan klęski żywiołowej