lic. Ewa Bielecka
Akademia Bialska im. Jana Pawła II

lic. Konrad Borówka
Akademia Bialska im. Jana Pawła II

lic. Oskar Szalej
Akademia Bialska im. Jana Pawła II

prof. dr hab. inż. Zbigniew Ciekanowski
Akademia Bialska im. Jana Pawła II
ORCID 0000-0002-0549-894X
https://doi.org/10.29316/9788368103199_9

ZAGROŻENIA INFRASTRUKTURY KRYTYCZNEJ JAKO WYZWANIA BEZPIECZEŃSTWA PAŃSTWA

THREATS TO CRITICAL INFRASTRUCTURE AS A CHALLENGE TO NATIONAL SECURITY

Streszczenie

Celem rozdziału jest identyfikacja i analiza współczesnych zagrożeń wobec infrastruktury krytycznej oraz wskazanie ich wpływu na bezpieczeństwo narodowe. Problem badawczy sformułowano: w jaki sposób zagrożenia wobec infrastruktury krytycznej wpływają na poziom bezpieczeństwa narodowego państwa? Wychodząc od teoretycznych podstaw pojęcia bezpieczeństwa, ukazano jego wielowymiarowość, a także znaczenie dla jednostki, społeczeństwa i państwa. Następnie omówiono

Summary

The aim of the chapter is to identify and analyze contemporary threats to critical infrastructure and to indicate their impact on national security. The research problem was formulated: how do threats to critical infrastructure affect the level of national security of the state? Starting from the theoretical foundations of the concept of security, its multidimensionality is shown, as well as its importance for the individual, society and the state. Then, social needs in the field of

społeczne potrzeby w zakresie bezpieczeństwa narodowego, podkreślając konieczność zapewnienia trwałości funkcjonowania państwa i jego instytucji. W dalszej części zaprezentowano definicje i istotę bezpieczeństwa narodowego oraz bezpieczeństwa wewnętrznego, a także dokonano klasyfikacji zagrożeń, dzieląc je na naturalne i cywilizacyjne. Szczególną uwagę poświęcono infrastrukturze krytycznej, ukazując jej kluczową rolę w stabilnym funkcjonowaniu państwa. Wskazano, że współczesne zagrożenia zwłaszcza w cyberprzestrzeni mają coraz większy wpływ na systemy infrastrukturalne. W rozdziale omówiono również konkretne przypadki cyberataków, m.in. na Estonię, Iran, Ukrainę i Grecję, obrazujące skalę i skutki takich incydentów. Zastosowano metody teoretyczne, takie jak analiza literatury, aktów prawnych oraz analiza przypadków (case study), co pozwoliło na sformułowanie głównego wniosku.

Słowa kluczowe: infrastruktura krytyczna, bezpieczeństwo narodowe, zagrożenia, cyberbezpieczeństwo, zarządzanie kryzysowe

national security were discussed, emphasizing the need to ensure the durability of the functioning of the state and its institutions. Further on, the definitions and essence of national security and internal security are presented, as well as the classification of threats, dividing them into natural and civilizational. Particular attention is paid to critical infrastructure, showing its key role in the stable functioning of the state. It was pointed out that contemporary threats, especially in cyberspace, have an increasing impact on infrastructure systems. The chapter also discusses specific cases of cyberattacks, m.in. on Estonia, Iran, Ukraine and Greece, illustrating the scale and effects of such incidents. Theoretical methods such as literature analysis, legal acts and case studies were used, which allowed the main conclusion to be formulated.

Keywords: critical infrastructure, national security, threats, cybersecurity, crisis management

Wstęp

Współczesne państwa funkcjonują w środowisku złożonym i dynamicznym, pełnym nieprzewidywalnych zagrożeń, które mogą w jednej chwili zakłócić porządek społeczny, gospodarczy czy polityczny. W dobie globalizacji, rozwoju technologicznego oraz rosnących napięć geopolitycznych pojęcie bezpieczeństwa nabiera coraz większego znaczenia, stając się kluczowym elementem polityki narodowej. Szczególną rolę w systemie bezpieczeństwa państwa odgrywa infrastruktura krytyczna – fundament nowoczesnego społeczeństwa, którego prawidłowe funkcjonowanie warunkuje stabilność i rozwój całego kraju.

W niniejszym opracowaniu autorzy podejmują próbę analizy istoty zagrożeń dla infrastruktury krytycznej oraz ich wpływu na bezpieczeństwo państwa. Przedstawione zostaną zarówno podstawowe definicje i uwarunkowania bezpieczeństwa narodowego, jak i konkretne zagrożenia – naturalne,

cywilizacyjne oraz cybernetyczne – które w sposób bezpośredni oddziałują na strategiczne systemy państwowe. Omówione zostaną również przykłady rzeczywistych incydentów z ostatnich lat, które ukazują, jak wrażliwa może być infrastruktura państw na celowe działania destrukcyjne.

Celem rozdziału jest wskazanie, że ochrona infrastruktury krytycznej nie jest wyłącznie zadaniem technicznym, ale złożonym procesem o wymiarze strategicznym, organizacyjnym i społecznym, który wymaga ciągłej adaptacji do zmieniających się warunków i zagrożeń. Tylko zintegrowane podejście pozwoli na skuteczne przeciwdziałanie sytuacjom kryzysowym i zapewnienie trwałego bezpieczeństwa państwa oraz jego obywateli.

Wprowadzenie do problematyki bezpieczeństwa

W dobie dzisiejszych kryzysów i konfliktów, pojęcie bezpieczeństwa zyskało na atrakcyjności, nie tylko w kwestii podejmowanych działań w celu osiągnięcia tego jakże pożądanego stanu, ale ciągłego usystematyzowania definicji wynikających z dynamiki pojawiających się zagrożeń.

Literatura przedmiotu zawiera wiele określeń bezpieczeństwa, wskazując jednocześnie na jego złożoność, interdyscyplinarność oraz wielowymiarowość podkreślając przy tym jego dynamiczny, wieloznaczny i wielopłaszczyznowy charakter[1]. Najczęściej termin bezpieczeństwo jest definiowany jako stan, w którym jednostka, grupa społeczna, organizacja czy państwo nie odczuwa zagrożenia dla swobodnego istnienia czy też realizacji podstawowych interesów,[2] jak również definiowane jest jako stan niezagrożenia, spokoju, pewności; stan i poczucie pewności, wolność od zagrożeń, strachu lub ataku[3]. Bezpieczeństwo ujmowane jest coraz częściej jako jedna z najważniejszych i zarazem podstawowych potrzeb współczesnego człowieka, jest to stan dający pewność, jak również jego trwanie i niezakłócony rozwój. Jego zasadniczą funkcją jest ochrona wartości i zasobów oraz korelacja zmian powstających w otoczeniu.

---

[1] Z. Trejnis, *Spory wokół określenia bezpieczeństwa* [w:] *Metodologia badań bezpieczeństwa narodowego*. *Bezpieczeństwo 2010*, red. P. Sienkiewicz, M. Marszałek, H. Świeboda, AON, Warszawa 2011, s. 363-370.

[2] *Słownik encyklopedyczny. Edukacja obywatelska,* Wydawnictwo Europa, Wrocław 2001, s. 44.

[3] J. Marczak, *Bezpieczeństwo Narodowe – pojęcie, charakter, uwarunkowania…,* op. cit., s. 7-8.

Bezpieczeństwo jest pojęciem szerokim, które jest ujmowane zarówno jako proces lub stan. W pierwszej kwestii jest dynamicznym, ulegającym przeobrażeniom procesem, w wyniku, którego zachodzą zmiany w organizacji i stanie bezpieczeństwa. W drugim przypadku zaś bezpieczeństwo ma charakter zależny od aktualnych incydentów, jest to stan spokoju, autonomii od wszelkich zagrożeń. Stan owego bezpieczeństwa jest zależnym od subiektywnego oraz obiektywnego dostrzegania poważnych niebezpieczeństw, co powoduje, że może ukazywać się pod różnymi postaciami. Brak bezpieczeństwa ma miejsce, gdy istnieje realne zagrożenie, obsesja natomiast związana jest z przesadnym dostrzeganiem zagrożeń, fałszywe bezpieczeństwo widnieje, gdy bagatelizowane są poważne zagrożenia, zaś stricte bezpieczeństwo, gdy prawidłowo odbierane jest niewielkie zagrożenie[4].

Specjaliści w swych rozważaniach są zgodni co do pojęcia bezpieczeństwa, które jest złożonym procesem, jak również, że oznacza autonomiczność od niebezpieczeństw dla fundamentalnych wartości w życiu każdego obywatela.

Interesującym elementem wpływającym na zwiększenie poczucia bezpieczeństwa jednostki/obywatela jest tzw. poczucie sprawstwa kojarzone najczęściej z przekonaniem o posiadanej wiedzy i umiejętnościach, które pozwolą zaradzić/zapanować w trudnej/kryzysowej sytuacji podczas wystąpienia nagłych i nieprzewidzianych zdarzeń.

Rozpoczynając postrzeganie potrzeby bezpieczeństwa należy zauważyć, że to samo zagadnienie przekłada się na społeczeństwo, jak również państwo. Potrzeby społeczeństwa w zakresie bezpieczeństwa narodowego precyzyjnie ujął J. Marczak jako powszechnie uświadomione i konieczne dążenie do przygotowania państwa na wszystkich szczeblach i we wszystkich dziedzinach jego organizacji do ciągłej i skutecznej ochrony i obrony interesów i wartości narodowych przed zagrożeniami militarnymi i niemilitarnymi, w warunkach niepewności i postępu – zapewniające przetrwanie narodu i jego wartości, pomyślność i dobrobyt oraz tworzenie warunków rozwoju dla obecnych i przyszłych pokoleń Polaków[5].

---

[4] Z. Ciekanowski, J. Nowicka, H. Wyrębek, *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń,* Wydawnictwo UPH, Siedlce 2016, s. 15.

[5] J. Marczak, *Społeczeństwo w tworzeniu bezpieczeństwa narodowego,* [w:] *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji,* red. R. Jakubczak, J. Marczak, K. Gąsiorek, W. Jakubczak, Warszawa 2008, s. 101.

Zatem katalog potrzeb społeczeństwa w zakresie bezpieczeństwa uwzględnia jego dwa podstawowe składniki - gwarancję nienaruszalnego przetrwania podmiotu oraz zapewnienie warunków do jego pełnego rozwoju. Potrzeby te dotyczą następujących obszarów[6]:

- bezpieczeństwa i porządku publicznego, a także sprawiedliwości;
- bezpieczeństwa powszechnego;
- ochrony zdrowia oraz bezpieczeństwa sanitarno-epidemiologicznego; ochrony środowiska i gospodarki odpadami;
- ochrony dorobku kulturowego i tożsamości narodowej; bezpieczeństwa ekonomicznego; oświaty i wychowania;
- bezpieczeństwa społecznego; bezpieczeństwa państwa;
- bezpieczeństwa międzynarodowego.

Biorąc pod uwagę aspekty, odnoszące się do przetrwania oraz niezakłóconego rozwoju jednostki, w tak przygotowanym katalogu potrzeb społeczeństwa należałoby uwzględnić potrzeby dotyczące ochrony infrastruktury krytycznej, co uczynił J. Marczak, formułując następujące rodzaje potrzeb społeczeństwa w zakresie bezpieczeństwa narodowego[7]:

- strategiczne potrzeby bezpieczeństwa narodowego;
- potrzeby świadomości, wiedzy i umiejętności z zakresu bezpieczeństwa narodowego;
- prawne i strukturalne potrzeby;
- potrzeby w zakresie bezpieczeństwa społecznego;
- potrzeby w zakresie bezpieczeństwa i porządku publicznego;
- potrzeby w zakresie ochrony infrastruktury krytycznej państwa;
- potrzeby w zakresie ochrony ludności i ratownictwa w sytuacji zagrożeń;
- potrzeby w sytuacjach zagrożeń.

J. Stańczyk użył trafnego określenia, które brzmi, iż istotą opartego na gwarancjach nienaruszalnego przetrwania i swobodach rozwojowych bezpieczeństwa, jest pewność[8]. Jest ona bowiem warunkiem obu tych składników, choć może być ona obiektywna lub subiektywna. Bezpieczeństwo w syntetycznym ujęciu można określić jako obiektywną pewność gwarancji nienaruszalnego

[6] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, op. cit., s. 31-32.

[7] J. Marczak, *Społeczeństwo w tworzeniu bezpieczeństwa narodowego,* [w:] *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji,* red. R. Jakubczak, J. Marczak, K. Gąsiorek, W. Jakubczak, Warszawa 2008, s. 101-106.

[8] J. Stańczyk, *Kres zimnej wojny*, Toruń 2004, s. 261.

przetrwania i swobód rozwojowych, które stanowi o losach narodu, społeczności oraz jednostki.

Na to składa się wiele przyczyn, z których najważniejsze należałoby uwzględnić podczas rozpatrywania problematyki bezpieczeństwa narodowego:

- pierwsza – to decydująca o losach jednostek i społeczeństw lokalnych - znaczenie narodu jako trwałej wspólnoty ludzi utworzonej historycznie, powstałej na gruncie wspólnoty losów, kultury, religii, języka, terytorium i życia gospodarczego, przejawiającego się w świadomości narodowej jej członków;
- druga – to znaczenie państwa narodowego jako najwyższej formy organizacyjnej narodu dla realizacji swych celów, z których priorytetem jest bezpieczeństwo narodowe;
- trzecia – to doświadczenia minionych wieków, wojen i zniszczeń, grabieży majątku narodowego i zniewolenia w różnych okresach[9].

Mówiąc o bezpieczeństwie narodowym należy przytoczyć jego definicję, która była wielokrotnie normowana. Definicja najbardziej odpowiadająca istocie współczesnego bezpieczeństwa narodowego, zawarta w Słowniku terminów z zakresu bezpieczeństwa narodowego, wydanym przez Akademię Obrony Narodowej w 2009 roku, której treść jest następująca: bezpieczeństwo narodowe - proces lub stan zapewniający funkcjonowanie (aktywność) państwa w podstawowych dziedzinach, umożliwiający przetrwanie, rozwój i swobodę realizacji interesów narodowych w konkretnym środowisku (warunkach) bezpieczeństwa, poprzez podejmowanie wyzwań, wykorzystywanie szans, redukowanie ryzyk oraz przeciwdziałanie wszelkiego rodzaju zagrożeniom dla jego interesów.

Bezpieczeństwo narodowe jest również interesem narodowym, utożsamianym z przetrwaniem państwa i narodu, ochroną granic oraz niezależności politycznej. Oprócz przetrwania, bezpieczeństwo ma za zadanie chronić także takie wartości jak: suwerenność, niezawisłość, przeżycie ludności, system społeczny i gospodarczy, prestiż w środowisku międzynarodowym, ideologię, własnych obywateli za granicą, postęp gospodarczy, standard życia ludności.

Bezpieczeństwo narodowe dosyć często bywa utożsamiane z bezpieczeństwem państwa, wynika to z faktu, że wywodzi się z egzystencjalnych potrzeb ludzkich społeczności zorganizowanych w państwa.

[9] R. Jakubczak, *Bezpieczeństwo narodowe Polski w XXI wieku*, Bellona, Warszawa, 2006, s. 17.

Bezpieczeństwo państwa jest integralnie powiązane z procesem powstawania nowoczesnych państwowości, powinno być postrzegane jako ciągły proces ulegający zmianom zarówno co do zasięgu, jak i jakości. Z punktu widzenia poruszanej problematyki najbardziej adekwatne jest postrzeganie bezpieczeństwa państwa jako stanu uzyskanego w wyniku zorganizowanej obrony i ochrony przed zagrożeniami zewnętrznymi i wewnętrznymi, określanego stosunkiem potencjału obronnego do skali zagrożeń[10].

Przed przedstawieniem definicji bezpieczeństwa wewnętrznego państwa należy również wyjaśnić, posługując się znaczeniem słownikowym, co oznacza pojęcie: *wewnętrzne*, które rozumieć należy jako: *znajdujący się, umieszczony we wnętrzu, w środku czegoś*[11]. I w tym miejscu należy się zatrzymać, aby wyjaśnić, jak należy rozumieć: w zamkniętej, ograniczonej czymś *przestrzeni, we wnętrzu czegoś*[12]. Przyjmując, że przedmiotem rozważań jest państwo i próba zdefiniowania słowa: *bezpieczeństwo wewnętrzne,* definicja dotyczyć będzie jednego z atrybutów państwa, czyli terytorium i społeczeństwa je zamieszkującego.

Wyniki przeprowadzonych dociekań pozwoliły na stwierdzenie, że bezpieczeństwo wewnętrzne państwa to stan uzyskany w efekcie spełniania przez państwo funkcji wewnętrznej, realizowanej w ramach strategicznej polityki bezpieczeństwa narodowego, przejawiający się ochroną:

- w ujęciu wąskim – porządku konstytucyjnego, bezpieczeństwa publicznego i bezpieczeństwa powszechnego;
- w ujęciu szerokim – porządku konstytucyjnego, życia i zdrowia obywateli, majątku narodowego przed bezprawnymi działaniami, a także skutkami klęsk żywiołowych i katastrof technicznych[13].

Przyczynami poczucia zagrożenia są dwa wyraźne źródła, a mianowicie natura i człowiek. Doświadczenia historyczne dowodzą, że największe zagrożenia dla człowieka stanowi drugi człowiek. Przyjmując przyczynę powstania zagrożeń, można podzielić je na dwie grupy[14]:

[10] B. Wiśniewski, J. Prońko, *Ogniwa ochrony …*, op. cit.

[11] Słownik języka polskiego, t. III, Wydawnictwo Naukowe PWN, Warszawa 1981, s. 682.

[12] Ibidem.

[13] B. Wiśniewski, *Zagrożenia bezpieczeństwa wewnętrznego, materiał na prawach maszynopisu*, Warszawa 2003.

[14] Z. Ciekanowski, H. Wyrębek, *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Wydawnictwo UPH, Siedlce 2016, s. 98.

a) zagrożenia naturalne – przypisane siłom natury, jako czynnik katastrof naturalnych, możemy je także podzielić na:
   - zagrożenia powszechne – to zagrożenie zwyczajne obecne, mają dostateczną regularnością powstawania katastrofalnych czynników jak np. generowanie hałasu komunikacyjnego o natężaniu przekraczającym podstawowe przedziały albo odprowadzanie zanieczyszczeń do wody, powietrza i gruntu;
   - zagrożenia nadzwyczajne – są to czynniki powodowane bodźcami naturalnymi lub cywilizacyjnymi, powodujące liczne zniszczenia przyrody, lub znaczne pogorszenie jej środowiska i mające wpływ na jakość życia ludności.

b) zagrożenia cywilizacyjne – odnoszące się do życia człowieka, mogące być impulsem powodującym katastrofy i awarie techniczne.

Do zdarzeń naturalnych należą[15]:

a) podtopienia (zimowe, roztopowe, zatorowo-lodowe, letnie, spowodowane awariami obiektów hydrotechnicznych);
b) sztormy;
c) duże wiatry i nawałnice;
d) nadmierne temperatury;
e) susze;
f) pioruny;
g) duże opady (deszczu, śniegu);
h) wstrząsy sejsmiczne (na określonych terenach);
i) kry na wodach otwartych;
j) choroby zakaźne ludzi i zwierząt;
k) rozmnażanie się gryzoni, owadów itp.;
l) lawiny i burze gradowe.

Do zagrożeń cywilizacyjnych należą[16]:

a) pożary (zabudowań, lasów, torfowisk, upraw rolnych);
b) katastrofy chemiczne;
c) awarie komunikacyjne;
d) zagrożenia środowiskowe i antropogeniczne;
e) zdarzenia budowlane;

[15] M. Lasoń, *Zagrożenia dla bezpieczeństwa Polski w XXI wieku w świetle analizy porównawczej kolejnych strategii Bezpieczeństwa Narodowej RP*, Bezpieczeństwo. Teoria i Praktyka, 2016, nr 3, s. 130.

[16] Ibidem, s. 131.

f) zdarzenia górnicze;
g) promieniowanie radiacyjne;
h) katastrofy infrastruktury technicznej;
i) działalność grup terrorystycznych;
j) skażenia promieniotwórcze;
k) zakażenia biologiczne ludzi, zwierząt i roślin.

Siły natury zagrażające bezpieczeństwu mogą powodować pożary, powodzie, osuwiska ziemi, anomalie pogodowe, które mogą doprowadzić do katastrof ekologicznych. Człowiek, występując przeciwko prawom przyrody, czy innemu człowiekowi, świadomie bądź nie, może przyczynić się do powstania zagrożeń skutkujących awariami technicznymi lub spowodować katastrofę ekologiczną. Zagrożeniami bezpieczeństwa publicznego w wyniku bezpośredniej działalności ludzi mogą być akty terroryzmu, konflikt zbrojny lub nawet wojna[17].

Człowiek nie zawsze działał w zgodzie z naturą, przeszłość pokazała również, że jego działalność była kierowana przeciwko innym ludziom. Takie sytuacje powodują zagrożenia również dla bezpieczeństwa publicznego. Pośrednio człowiek obsługując urządzenia przemysłowe, energetyczne, chemiczne, itp. poprzez swoje zaniedbania, bądź też w wyniku awarii tych urządzeń, powoduje sytuacje zagrażające bezpieczeństwu ludzi i środowiska.

Opracowania poświęcone zagadnieniom zagrożenia bezpieczeństwa państwa posługują się częstokroć takimi pojęciami jak kryzys, sytuacja kryzysowa, jak również zarządzanie kryzysowe. Podkreślana jest także konieczność przeciwdziałania tym sytuacjom, które powstają w sposób nagły, nieprzewidziany, ale wymagający reakcji w krótkim przedziale czasowym, gdyż kumulowanie i nierozwiązanie na czas, może prowadzić do zaistnienia sytuacji kryzysowych[18].

[17] J. Święcicki, *Ogólne zasady przygotowania sił i środków cywilnej służby zdrowia do ratowania zdrowia i życia ludzi w sytuacjach nadzwyczajnych i w czasie wojny*, Warszawa 2002, s. 50.

[18] K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Bel Studio, Warszawa 2007, s. 76.

Infrastruktura krytyczna jako cel zagrożeń

Poważne niebezpieczeństwo stanowią zagrożenia infrastruktury krytycznej. Do najczęściej występujących zagrożeń z tego zakresu można zaliczyć awarie:

- sieci ciepłowniczych,
- sieci energetycznych,
- sieci wodnokanalizacyjnych,
- sieci gazowych,
- urządzeń gazowych.

To właśnie technika jest najważniejszym i największym impulsem napędowym cywilizacji. Nowe wynalazki ułatwiają nam życie, ale stanowią również nowe zagrożenia, przez co czujemy się mniej bezpieczni. Cuda technologii mogą zarazem ułatwiać i utrudniać nasze życie, wpływać znacząco na stan bezpieczeństwa, zachwiać równowagą ekologiczną biosfery, a co ważne, oddziaływać na kształt życia społecznego. Pojawiają się ciągle nowe zagrożenia zwane cywilizacyjnymi.

Zapewnienie bezpieczeństwa obywatelom jest najważniejszym zadaniem każdego państwa. Realizacja tego zadania polega przede wszystkim na ochronie infrastruktury krytycznej. Każde powstałe zagrożenie mogące wywołać sytuację kryzysową ma wpływ na właściwe funkcjonowanie całego państwa oraz bezpośrednio przekłada się na jego bezpieczeństwo. Sytuacja kryzysowa rozumiana jako splot gwałtownych zdarzeń, które destabilizują równowagę w normalnym funkcjonowaniu społeczeństwa i prowadzą do niekontrolowanego rozwoju zdarzeń, zawsze dotyczyć będzie infrastruktury. To właśnie infrastruktura pozwala na istnienie państwa oraz jego poprawne funkcjonowanie, zaś jej kluczowe elementy tworzą infrastrukturę krytyczną.

Wraz z rozwojem cywilizacyjnym wzrasta uzależnienie społeczeństwa od właściwego funkcjonowania infrastruktury krytycznej. Rozwój ten wiąże się także z zachodzącymi przemianami, które przyczyniają się w sposób znaczący do powstawania nowych zagrożeń i ciągłym poszukiwaniem skutecznych rozwiązań w stabilizacji powiązanych ze sobą systemów, które wchodzą w skład infrastruktury krytycznej. Według ustawy o zarządzaniu kryzysowym, infrastruktura krytyczna to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej,

a także instytucji i przedsiębiorców[19]. Infrastruktura krytyczna odnosi się do systemów fizycznych i wirtualnych, które stanowią podstawę nowoczesnych społeczeństw i są niezbędne do ich przetrwania. Zgodnie z ustawą o zarządzaniu kryzysowym obejmuje systemy:

a) zaopatrzenia w energię, surowce energetyczne i paliwa;
b) łączności;
c) sieci teleinformatycznych;
d) finansowe;
e) zaopatrzenia w żywność;
f) zaopatrzenia w wodę;
g) ochrony zdrowia;
h) transportowe;
i) ratownicze;
j) zapewniające ciągłość działania administracji publicznej;
k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[20].

Zapewnienie bezpieczeństwa tych systemów jest kluczowym elementem strategii bezpieczeństwa narodowego współczesnych państw. Bezpieczne i efektywne zarządzanie infrastrukturą krytyczną jest wskaźnikiem dobrobytu społecznego oraz poziomu rozwoju gospodarczego danego kraju. Jest określana jako krytyczna, gdy zakłada się, że zakłócenie jej funkcjonowania może prowadzić do poważnego kryzysu społeczno-ekonomicznego, który ma potencjał podważenia stabilności społeczeństwa, a tym samym wywołania konsekwencji politycznych, strategicznych i związanych z bezpieczeństwem. Różne kraje mają różne definicje infrastruktury krytycznej. Wspólnym elementem wszystkich tych definicji jest obecność skomputeryzowanego komponentu, od którego zależą inne systemy fizyczne, a którego uszkodzenie może spowodować szeroko zakrojone straty materialne. Ochrona tych systemów przed cyberatakami, terroryzmem, awariami czy naturalnymi katastrofami jest niezbędna do utrzymania stabilności społeczeństw. Infrastruktura krytyczna obejmuje m.in. sieci energetyczne, wodociągowe, transportowe, systemy telekomunikacyjne oraz bankowe, które są fundamentem funkcjonowania państw. Jej integracja z nowoczesnymi technologiami sprawia, że jest narażona na nowe zagrożenia,

[19] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, art. 3, ust. 2.
[20] Ibidem.

wymagające ciągłego monitorowania, wzmocnionej obrony oraz rozwoju strategii ochrony przed cyberzagrożeniami[21].

Najistotniejszym elementem infrastruktury krytycznej jest skomputeryzowany komponent, od którego zależą inne systemy fizyczne w państwie, a którego zniszczenie może spowodować ogromne straty materialne. Istnieją trzy kluczowe czynniki definiujące infrastrukturę krytyczną[22]:

1) Wiele demokratycznych krajów uznaje obiekty dziedzictwa narodowego, muzea, archiwa i pomniki za część infrastruktury krytycznej, którą należy chronić przed zagrożeniami cybernetycznymi. Innym źródłem symbolicznej siły jest kontrola rządowa nad mediami. Na przykład, wrogie zakłócenie tradycyjnych mediów wykorzystywanych przez państwo do komunikacji z obywatelami, natychmiast osłabiłoby zdolność rządu do działania. Na dłuższą metę mogłoby to również podważyć zaufanie obywateli do obecnych władz, a nawet całego systemu politycznego.
2) Niektóre systemy, takie jak sieć energetyczna czy sieć telekomunikacyjna, są kluczowe dla większości procesów społecznych. Rozwój i powszechność cyberprzestrzeni sprawiły, że sieci skomputeryzowane stały się infrastrukturą samą w sobie. Cyberprzestrzeń to przykład infrastruktury, która stała się krytyczna ze względu na powiązanie większości aktywności społecznej z sieciami komunikacji cyfrowej.
3) Szybki rozwój technologii i ich łączności powoduje nieprzewidywalne efekty na szeroką skalę (tzw. „efekt motyla"). Relacje między różnymi infrastrukturami nie są w pełni poznane, a awaria jednego komponentu może prowadzić do szeregu dalszych zakłóceń i strat.

Obecnie bezpieczeństwo infrastruktury krytycznej w dużym stopniu zależy od technologii sieciowych, dlatego zapewnienie jej cyberbezpieczeństwa jest równoznaczne z ochroną bezpieczeństwa narodowego. Ochrona infrastruktury krytycznej przed cyberatakami jest kluczowa dla utrzymania codziennego funkcjonowania społeczeństwa, ponieważ gwarantuje dostęp do podstawowych usług publicznych oraz zapewnia stabilność transakcji handlowych i finansowych. Proces zarządzania infrastrukturą krytyczną za pomocą technologii sieciowych, które są głównie obsługiwane przez systemy mechaniczne pod nadzorem człowieka, przyspieszył od 1990 roku wraz z gwałtowną komercjalizacją i demilitaryzacją internetu, pod przewodnictwem Stanów

[21] L. Tabansky, *Critical Infrastructure Protection against Cyber Threats*, Military and Strategic Affairs, Vol 3. No. 2, 2011, s. 61-62.

[22] Ibidem, s. 63-64.

Zjednoczonych. W tym samym okresie zaczęto opracowywać strategie cyberbezpieczeństwa na poziomie krajowym i międzynarodowym. Obecnie wiele państw w systemie międzynarodowym posiada zdolności w zakresie obrony i ataku cybernetycznego, odpowiadające ich poziomowi rozwoju i potencjałowi gospodarczemu. Od początku XXI w. kraje dążą do udoskonalania swoich zdolności ofensywnych w cyberprzestrzeni na różne sposoby, m.in. poprzez szpiegostwo kosmiczne i kontrwywiad, rozpowszechnianie dezinformacji za pośrednictwem platform internetowych, rozwój umiejętności prowadzenia wojny elektronicznej, zarządzanie percepcją społeczną oraz szerzenie propagandy. Oprócz państw, wiele organizacji międzynarodowych i przedsiębiorstw opracowało plany dotyczące cyberbezpieczeństwa w ramach swojej działalności, dostosowując je do własnych celów strategicznych[23].

Cyberataki na infrastrukturę krytyczną – studium przypadku

Istnieje wiele konkretnych przykładów cyberataków wymierzonych w infrastrukturę krytyczną różnych państw. Wiele z nich miało miejsce po roku 2000, zanim rozwinięto pełną świadomość dotyczącą tego rodzaju zagrożeń. Pod koniec zimnej wojny napięcie między Rosją a Estonią wzrosło w wyniku zbliżenia Estonii do Sojuszu Północnoatlantyckiego (NATO). Sytuacja zaostrzyła się jeszcze bardziej po decyzji Estonii o usunięciu sowieckiego pomnika z Placu Tallinna. Bezpośrednio po tej decyzji kraj padł ofiarą szeroko zakrojonego ataku typu Distributed Denial of Service (DDoS), wymierzonego w infrastrukturę krytyczną Estonii. Celem ataków było sparaliżowanie estońskiego sektora internetowego poprzez unieruchomienie stron internetowych partii politycznych, instytucji państwowych, parlamentu, mediów, banków i systemu finansowego. W efekcie sektor internetowy infrastruktury krytycznej Estonii stał się niezdatny do użytku przez tydzień. Estonia odzyskała kontrolę nad sytuacją dzięki pomocy NATO oraz decyzji o czasowym zamknięciu dostępu do estońskiej sieci krajowej z zagranicy[24].

W czerwcu 2010 roku przeprowadzono cyberatak z wykorzystaniem wirusa Stuxnet na irański ośrodek jądrowy w Natanz. Wirus ten spowodował

[23] A. Burak, *National Security 2.0: The Cyber Security of Critical Infrastructure*, Perceptions: Journal of International Affairs, 2021, 26(2), s. 260.

[24] M. Czepielewski, *Cyberterroryzm jako element społeczeństwa informacyjnego (na przykładzie Estonii),* [w:] *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. T. Jemioła, Wydawnictwo Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa 2009, s. 178-188.

fizyczne uszkodzenie instalacji i opóźnił rozwój irańskiego programu nuklearnego. Chociaż Iran oskarżył Stany Zjednoczone i Izrael o przeprowadzenie ataku, żadna ze stron oficjalnie nie przyznała się do jego przeprowadzenia. Stuxnet był pierwszym znanym przykładem użycia cyberbroni do uszkodzenia infrastruktury krytycznej, zainfekował systemy sterujące wirówek jądrowych, powodując ich awarie i dezinformując operatorów[25].

23 grudnia 2015 roku ukraiński operator dystrybucji energii Prykarpattya Oblenergo padł ofiarą cyberataku wymierzonego w jego infrastrukturę ICT (technologie informacyjno-komunikacyjne). W wyniku tego incydentu doszło do zakłóceń w funkcjonowaniu kilku podstacji energetycznych, co spowodowało przerwę w dostawie prądu dla około 80 tysięcy mieszkańców regionu Iwano-Frankiwskiego. Według oficjalnych informacji podanych przez operatora, awaria trwała od trzech do sześciu godzin. Równocześnie doszło do awarii systemu centrum obsługi klienta, co uniemożliwiło mieszkańcom kontakt z operatorem i zgłaszanie problemów. To dodatkowo pogłębiło kryzys i utrudniło koordynację działań naprawczych. Analiza zdarzenia wskazuje, że był to dobrze skoordynowany cyberatak, składający się z trzech głównych elementów[26]:

- Hakerzy zainfekowali główne serwery kontrolujące dystrybucję energii elektrycznej. Prawdopodobnie wykorzystali do tego backdoor malware, który pozwolił im uzyskać dostęp do sieci operatora i wysłać polecenie otwarcia wyłączników w kilku podstacjach, co doprowadziło do przerw w dostawie prądu.
- Złośliwe oprogramowanie zostało rozprzestrzenione poprzez spreparowane pliki Excel zawierające makra, które były wysyłane w ramach kampanii spear-phishingowej. Atakujący kierowali swoje wiadomości do pracowników IT i administratorów systemów pracujących w firmach odpowiedzialnych za dystrybucję energii elektrycznej na Ukrainie.
- Po wyłączeniu prądu hakerzy przeprowadzili atak DoS na systemy obsługi klienta, blokując możliwość kontaktu mieszkańców z operatorem. Spowodowało to, że personel techniczny nie otrzymywał informacji zwrotnych na temat skutków ataku, co opóźniło reakcję kryzysową i przywrócenie dostaw energii.

[25] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni: zagrożenia i wyzwania dla Polski – zarys problemu*, Kwartalnik BN: Strategiczne doświadczenia Polski w NATO i UE, 2012, nr 22, s. 135.

[26] M. Choraś, *Cyber Threats Impacting Critical Infrastructures*, [w:] Managing the Complexity of Critical Infrastructures, red. R. Setola, Wydawnictwo Springer Open, 2017.

Atak na ukraińską sieć energetyczną był jednym z pierwszych znaczących cyberataków wymierzonych bezpośrednio w infrastrukturę cywilną. W przeciwieństwie do wcześniejszych przypadków, takich jak Stuxnet, który był wymierzony w instalacje przemysłowe i wojskowe, tutaj ofiarą była bezpośrednio ludność cywilna. Atak ten pokazał, że cyberprzestępcy są w stanie powodować poważne szkody gospodarcze i zagrożenia dla bezpieczeństwa publicznego państw. W przypadku Ukrainy infrastruktura nadal umożliwiała ręczne przywracanie zasilania, co pozwoliło na stosunkowo szybkie przywrócenie energii. Jednak w bardziej nowoczesnych i zautomatyzowanych systemach energetycznych, gdzie zarządzanie siecią opiera się na pełnej cyfryzacji, skutki takiego ataku mogłyby być znacznie poważniejsze[27].

Kolejnym wartym uwagi przykładem jest atak na infrastrukturę w Grecji. 20 sierpnia 2022 roku, grecka organizacja odpowiedzialna za obsługę, zarządzanie, eksploatację i rozwój krajowego systemu gazu ziemnego (NNGS) oraz jego połączeń, ujawniła atak cybernetyczny na część swojej infrastruktury informacyjnej. Cyberprzestępcy próbowali nielegalnie uzyskać dostęp do plików elektronicznych, co skutkowało potwierdzonym wpływem na dostępność niektórych systemów oraz potencjalnym wyciekiem plików i danych. W odpowiedzi organizacja proaktywnie wyłączyła większość swoich usług infrastruktury informacyjnej i zdecydowała się na stopniowe przywracanie systemów, wybierając opcję braku negocjacji z cyberprzestępcami[28].

Przykład ukraiński daje krótkie spojrzenie na możliwe skutki udanego cyberataku wymierzonego w krytyczną infrastrukturę, taką jak sieć energetyczna. Niestety, z powodu obecnej sytuacji geopolitycznej oraz współczesnego rynku hackerów (państwowych i niepaństwowych) istnieje istotne zagrożenie, że kraj lub jego krytyczna infrastruktura mogą zostać zaatakowane przez inne państwo lub organizację hakerską działającą na rzecz wrogiego kraju. Warto zauważyć, że obecnie większość hackerów pracuje dla organizacji, a nie na własny rachunek. Inaczej mówiąc, cyberataki mogą być częścią tzw. wojny hybrydowej lub konfliktu hybrydowego, gdzie (przynajmniej na pierwszych etapach) tradycyjne środki militarnego oddziaływania (takie jak żołnierze) nie są używane, a koncentracja przenosi się na inne destabilizujące aspekty, takie jak cyberataki, cyberpropaganda, wpływanie na media społecznościowe i media elektroniczne itd. Jeśli najgorsze scenariusze staną się rzeczywistością,

[27] Ibidem, 143.

[28] K. Mitsarakis, *Contemporary Cyber Threats to Critical Infrastructures: Management and Countermeasures,* Wydawnictwo IHU, 2023, s. 9.

udane, skoordynowane cyberataki wymierzone w krytyczne infrastruktury, takie jak banki, energia, transport, media itd., mogą sparaliżować społeczeństwa, kraje i wywołać chaos. Dlatego, aby uniknąć sytuacji podobnej do tej na Ukrainie, konieczne są skuteczne rozwiązania i technologie służące ochronie systemów cyberfizycznych. Opracowane rekomendacje i technologie powinny obejmować szeroki zakres aspektów, takich jak technologiczne, organizacyjne, ludzkie i regulacyjne[29].

Ocena ilościowa bezpieczeństwa cybernetycznego zawsze stanowi wyzwanie w obszarze informatyki. Dla systemów cyberfizycznych integracja technologii ICT z elementami fizycznymi wprowadziła nowe zagrożenia. Obecnie możemy znaleźć wiele przykładów, w których atakujący byli w stanie skompromitować złożone systemy, znajdując podatne elementy. W wielu przypadkach te ataki miały bezpośredni wpływ na elementy fizyczne. W związku z tym trwają starania, aby objąć aspekty cybernetyczne kompleksowymi narzędziami i metodologiami, które zwykle wykorzystują szeroki wachlarz środków technicznych i nietechnicznych. Obecne wyzwania związane z systemem cyberfizycznym można podzielić na następujące grupy problemów[30]:

- bezpieczeństwo,
- skalowalność,
- złożoność,
- wzajemna zgodność subsystemów.

Oczywiście takie problemy powinny być rozwiązywane w sposób holistyczny, np. za pomocą podejścia THOR (Techniczne, Ludzkie, Regulacyjne, Organizacyjne) i aspektów zaproponowanych przez niedawno zakończone projekty europejskie, ponieważ bezpieczeństwo cybernetyczne systemów cyberfizycznych stanowi istotne wyzwanie[31].

Podsumowanie

Podsumowując proces globalizacji, powszechnego rozwoju technologicznego czy terroryzm znacząco wpływają na postrzeganie zagrożeń mających wpływ na bezpieczeństwo państwa. Rozwój nowoczesnych technologii, nie tylko w sposób pozytywny przyczynia się do rozwoju państw, co przekłada

[29] M. Choraś, *Cyber Threats Impacting Critical Infrastructures*, [w:] Managing the Complexity of Critical Infrastructures, red. R. Setola, Wydawnictwo Springer Open, 2017.

[30] Ibidem, s. 143-146.

[31] Ibidem.

się na jakość życia obywateli, ale wpływa na coraz szybsze powstawanie zagrożeń, z którymi państwo nie zawsze jest w stanie sobie poradzić. Uszkodzenie infrastruktury, jak również chwilowe zakłócenie, może doprowadzić do uszkodzenia pozostałych systemów, co w dalszej konsekwencji doprowadzi zachwiania bezpieczeństwa państwa. Systemy będące podatne na uszkodzenia wymagają stałej kontroli oraz ochrony ze strony państwa. Zagrożenia infrastruktury, które wraz z rozwojem cywilizacyjno-technologicznym stale ulegają zmianom muszą podlegać ciągłej klasyfikacji na podstawie kryteriów zagrożeń.

Literatura

1. Burak, A., *National Security 2.0: The Cyber Security of Critical Infrastructure*, Perceptions: Journal of International Affairs, 2021, 26(2).
2. Choraś M., Cyber *Threats Impacting Critical Infrastructures*, [w:] Managing the Complexity of Critical Infrastructures, red. R. Setola, Wydawnictwo Springer Open, 2017.
3. Ciekanowski Z., Wyrębek H., *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Wydawnictwo UPH, Siedlce 2016.
4. Czepielewski M., *Cyberterroryzm jako element społeczeństwa informacyjnego (na przykładzie Estonii)*, [w:] *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. T. Jemioła, Wydawnictwo Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa 2009, s. 178-188.
5. Ficoń K., *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Bel Studio, Warszawa 2007.
6. Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni: zagrożenia i wyzwania dla Polski – zarys problemu*, Kwartalnik BN: Strategiczne doświadczenia Polski w NATO i UE, 22, 2012, s. 125-139.
7. Jakubczak R., *Bezpieczeństwo narodowe Polski w XXI wieku*, Bellona, Warszawa, 2006.
8. Lasoń M., *Zagrożenia dla bezpieczeństwa Polski w XXI wieku w świetle analizy porównawczej kolejnych Strategii Bezpieczeństwa Narodowej RP*, Bezpieczeństwo. Teoria i Praktyka, nr 3, 2016, s. 123-137.
9. Marczak J., *Społeczeństwo w tworzeniu bezpieczeństwa narodowego*, [w:] *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji*, red. Jakubczak R., Marczak J., Gąsiorek K., Jakubczak W., Warszawa 2008.
10. Mitsarakis M., C*ontemporary Cyber Threats to Critical Infrastructures: Management and Countermeasures*, Wydawnictwo IHU, 2023.
11. Słownik encyklopedyczny. Edukacja obywatelska, Wydawnictwo Europa, Wrocław 2001.
12. Słownik języka polskiego, T. III, Wydawnictwo Naukowe PWN, Warszawa 1981.
13. Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Instytut Studiów Politycznych PAN, Warszawa. 1996.

14. Stańczyk J., *Kres zimnej wojny*, Toruń 2004.
15. Święcicki J., *Ogólne zasady przygotowania sił i środków cywilnej służby zdrowia do ratowania zdrowia i życia ludzi w sytuacjach nadzwyczajnych i w czasie wojny*, Warszawa 2002.
16. Tabansky L., *Critical Infrastructure Protection against Cyber Threats*, "Military and Strategic Affairs, 3(2), 2011, 61-78.
17. Trejnis Z., *Spory wokół określenia bezpieczeństwa*, [w:] *Metodologia badań bezpieczeństwa narodowego*, red. Sienkiewicz P., Marszałek M., Świeboda H., AON, Warszawa 2021.
18. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89, poz. 59).
19. Wiśniewski B., *Zagrożenia bezpieczeństwa wewnętrznego, materiał na prawach maszynopisu*, Warszawa 2003.