Akademia Bialska im. Jana Pawła II



Wielowymiarowość środowiska bezpieczeństwa

Redakcja naukowa
Dariusz Brążkiewicz
Marta Chodyka
Tomasz Grudniewski
Julia Nowicka

Część pierwsza

AKADEMIA BIALSKA
IM. JANA PAWŁA II
Jubileusz 25-lecia

Wielowymiarowość środowiska bezpieczeństwa

Część pierwsza

Redakcja naukowa

Dariusz Brążkiewicz
Marta Chodyka
Tomasz Grudniewski
Julia Nowicka

Biała Podlaska 2025

Wydawca
Akademia Bialska im. Jana Pawła II

Recenzenci
prof. dr hab. inż. Marian Kopczewski, Akademia Wojsk Lądowych
dr hab. inż. Henryk Wyrębek, prof. uczelni, Uniwersytet w Siedlcach

Korekta językowa
mgr Marzanna Brążkiewicz

© Copyright by Akademia Bialska im. Jana Pawła II

Książka jest udostępniana na licencji Creative Commons Uznanie autorstwa – Użycie niekomercyjne – Bez utworów zależnych 4.0 Międzynarodowa

ISBN 978-83-68103-19-9
https://doi.org/10.29316/9788368103199

Nakład: 80 egzemplarzy

Wydawnictwo AB JPII
ul. Sidorska 95/97
21-500 Biała Podlaska
wydawnictwo.akademiabialska.pl

Projekt okładki, skład i druk

druk-24h.com.pl
DRUKARNIA CYFROWA
Hurtowa 21, 15-399 Białystok
tel. 535 500 898
e-mail: studio@druk-24h.com.pl

Spis treści

Wstęp 5

Aneta Kułakowska
Usytuowanie paradygmatu geopolityki w bezpieczeństwie państwa . . 9

Anna Opar
Współczesne zagrożenia bezpieczeństwa. Terroryzm 29

Łukasz Szymankiewicz
Proces radykalizacji a terroryzm – casus baskijskiej organizacji terrorystycznej ETA 47

Iwona Lasek-Surowiec, Bartosz Błaszczak, Irena Malinowska, Marcin Oskierko
Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu w zwalczaniu terroryzmu na poziomie krajowym i międzynarodowym 65

Dariusz Brążkiewicz, Rafał Mazurek
Współczesne powietrzne drony rozpoznawczo-bojowe i ich użycie oraz zwalczanie na przykładzie wojny rosyjsko-ukraińskiej 81

Barbara Stefaniuk
Cyberterroryzm jako zagrożenie bezpieczeństwa globalnego 105

Marta Chodyka
Bezpieczeństwo baz danych jako element odporności cybernetycznej sił zbrojnych 123

Tomasz Grudniewski
Zaawansowane systemy fotowoltaiczne jako kluczowy czynnik wzmacniający bezpieczeństwo energetyczne państwa 141

Ewa Bielecka, Konrad Borówka, Oskar Szalej, Zbigniew Ciekanowski
Zagrożenia infrastruktury krytycznej jako wyzwania bezpieczeństwa państwa 163

Marta Chodyka
Bezpieczeństwo systemów informatycznych a funkcjonowanie przedsiębiorstw w Polsce 181

Mariusz Czternastek, Sławomir Żurawski, Marek Chwała, Patryk Ochyra
Państwowa Straż Pożarna jako istotny element zarządzania kryzysowego podczas wystąpienia powodzi 209

Tomasz Grudniewski
Integracja fotowoltaiki wspieranej sztuczną inteligencją w strategiach bezpieczeństwa energetycznego państw 227

Jerzy Bertrandt, Justyna Bandura, Karolina Bertrandt-Tomaszewska
Otyłość – współczesne zagrożenie bezpieczeństwa zdrowotnego . . . 251

Zdzisław Małkowski, Zbigniew Skwarek, Piotr Waniek, Andrzej Skonieczny
Rola organizacji pozarządowych w zapewnieniu bezpieczeństwa humanitarnego uchodźcom w Polsce 273

Beata Spinek, Malwina Olbrych, Waldemar Perdion, Sławomir Żurawski
Wpływ infrastruktury drogowej na bezpieczeństwo w ruchu drogowym 287

Zbigniew Piskor
Zarządzanie zasobami załogi lotniczej 303

Martyna Zaroślak
Commercial sharenting jako zagrożenie dobrostanu dziecka 321

Magdalena Miczek
Kształtowanie postaw jako jeden z filarów bezpieczeństwa państwa 343

WSTĘP

Współczesne wyzwania cywilizacyjne i zmieniające się środowisko bezpieczeństwa w wymiarze międzynarodowym i wewnętrznym kształtują obecną świadomość narodów, społeczeństw oraz grup religijno-etnicznych. Jednym z głównych aspektów jest postępująca globalizacja w postaci postępu cywilizacyjnego, trendów światowych, rozwoju nowoczesnych technologii wyznaczających tempo i kierunek zmian, które niosą ze sobą oprócz wielu pozytywnych elementów, również te negatywne. Dla skutecznego przeciwdziałania współczesnym zagrożeniom, niezbędne jest całościowe podejście do bezpieczeństwa zarówno w skali lokalnej, narodowej, jaki i międzynarodowej. Tym samym państwo, by mogło osiągnąć określony stopień bezpieczeństwa, podejmuje szereg różnorodnych działań, w tym analizę ryzyka geopolitycznego.

Od wielu lat jednym z największych zagrożeń jest terroryzm, a przyczyną tego zjawiska są m.in. następujące motywy: polityczne, ideologiczne, narodowościowe, religijne oraz społeczne. Terroryzm nie jest zjawiskiem jednorodnym i jego nasilenie jest różne w czasie i miejscu występowania. Dość wyraźnie terroryzm kojarzy się głównie z aspektami religijnymi, wynikającymi z przenikania się we współczesnym świecie kultur i przyjmowania odmiennych, cywilizacyjnych wzorców we współczesnych społeczeństwach, nieakceptowanych przez wiele grup społecznych w poszczególnych państwach z radykalną, ortodoksyjną religią. Terror jest również narzędziem grup i gangów przestępczych, trudniących się handlem narkotykami i ludźmi. Do walki z tymi zjawiskami państwa używają instytucji i agencji wywiadowczych, zdolnych do permanentnej inwigilacji i rozbijania tych środowisk, będących jednym z głównych zagrożeń bezpieczeństwa wewnętrznego państwa.

Nadal wzrasta również zagrożenie wynikające z ataków cybernetycznych. Postępująca transformacja cyfryzacji generuje kolejne cyberzagrożenia. Są to zagrożenia systemowe, jak i incydentalne. W przypadku zagrożeń systemowych, potrzebne są coraz nowocześniejsze systemy informatyczne odporne na takie zagrożenia. W przypadku zagrożeń incydentalnych, to w przeważającej części dotyczą one ataków na wybrane osoby, celem wyłudzenia danych, a co za tym idzie, finansów. Uwarunkowania te wskazują na potrzebę działań

systemowych ochrony instytucji i obywateli, ze szczególnym elementem ciągłej poprawy świadomości powstających kolejnych zagrożeń. Jednocześnie nie jest to problem wybranych państw, lecz wielu, a obejmując swoim zasięgiem cały świat, wskazuje, że jest to zjawisko globalne i zagrożenie cybernetyczne może płynąć nawet z drugiej strony globu.

Współczesna cyfryzacja i miniaturyzacja dość wyraźnie, a właściwie bardzo mocno wpływa na współczesne pole walki w konfliktach zbrojnych. Przykładem tego jest trwająca wojna rosyjsko-ukraińska, gdzie współczesne powietrzne drony rozpoznawczo-bojowe są jednym z głównych zagrożeń dla walczących stron. Różnorodność wielkości powietrznych dronów pozwala na różne ich użycie, proporcjonalnie do możliwości i planowanych potrzeb. Ich adaptacja do warunków bojowych ma wiele aspektów, ale możliwości wykorzystania zdecydowanie zmieniły zasady walki w pełnoskalowym konflikcie. Masowe użycie dronów bojowych o niskich kosztach produkcji pozwala na eliminację bardzo drogiego uzbrojenia i sprzętu przeciwnika. Tym samym kilka ostatnich lat przyniosło rewolucję w sposobie prowadzenia działań bojowych na współczesnym polu walki.

Wyzwania wewnętrznego bezpieczeństwa państwa mają swoje odzwierciedlenie w zarządzaniu kryzysowym. Dotyczy to infrastruktury krytycznej, jak i katastrof naturalnych, pojawiających się regularnie co kilka lat. W przypadku infrastruktury krytycznej, to wszelkie działania ochronne przed zagrożeniami są domeną państwa. W przypadku katastrof naturalnych, takich jak powodzie, bardzo ważne miejsce zajmuje Państwowa Straż Pożarna. W obu tych obszarach ważne jest zgranie służb posiadających narzędzia do niwelowania lub naprawiania szkód oraz czas reakcji na zaistniałe incydenty. W ramach zgrywania służb, bardzo ważne miejsce zajmuje wojsko, mające możliwości techniczne i ludzkie, w interwencyjnych działaniach na rzecz państwa i obywateli. Ponadto nieodzowna jest współpraca administracji rządowej i samorządowej, które są jednymi z najważniejszych ogniw w realizacji działań ratowniczych w sytuacjach kryzysowych.

Jednym z ważnych aspektów współczesnego bezpieczeństwa państwa i obywateli jest możliwość pozyskiwania energii z odnawialnych źródeł energii. Od wielu lat rozwija się przemysł systemów fotowoltaicznych do wykorzystania masowego, na dużych farmach oraz domowego, przez odbiorców indywidualnych. To odnawialne źródło energii słonecznej, pozwala na zwiększenie bezpieczeństwa energetycznego poprzez dywersyfikację źródeł i uniezależnienie się od importowanych surowców kopalnych. Tym samym

dynamiczny rozwój technologii fotowoltaicznych w ostatnich latach doprowadził do powstania szeregu zaawansowanych rozwiązań, które charakteryzują się wyższą wydajnością i stabilnością pracy. Tworzenie bezpieczeństwa energetycznego to nie tylko kwestia geopolityki dostaw, ale także zdolność do pokrycia krajowego zapotrzebowania na energię w sposób ciągły, nawet w sytuacjach nadzwyczajnych.

Monografia stanowi szeroki przegląd wiedzy autorów o bezpieczeństwie w środowisku globalnym i regionalnym oraz krajowym. Poszczególne rozdziały stanowią wynik prowadzonych przez autorów analiz wielu aspektów związanych z wyzwaniami i zagrożeniami bezpieczeństwa. Przedstawione badania bezpieczeństwa zewnętrznego i wewnętrznego państwa oraz aspektów bezpieczeństwa społecznego państwa, dokonane zostały przez wieloletnich badaczy, jak i początkujących adeptów nauki. Różnorodność tematów wskazuje na szeroki zakres badań realizowanych w naukach o bezpieczeństwie oraz fakt, że większość rozważań dotyczy aspektów bezpieczeństwa państwa. Tym samym, ta różnorodność powinna stanowić ciekawą lekturę prezentowanych tematów.

bryg. dr Aneta Kułakowska
Akademia Pożarnicza
ORCID: 0000-0003-1829-568X
https://doi.org/10.29316/9788368103199_1

USYTUOWANIE PARADYGMATU GEOPOLITYKI W BEZPIECZEŃSTWIE PAŃSTWA

THE LOCATION OF THE GEOPOLITICAL PARADIGM IN STATE SECURITY

Streszczenie

Celem rozdziału jest identyfikacja roli, jaką geopolityka odgrywa w kształtowaniu strategii państw na rzecz zapewnienia ich bezpieczeństwa w obliczu globalnych zagrożeń. Problem badawczy sformułowano: jakie znaczenie ma geopolityka jako paradygmat dla bezpieczeństwa państwa w warunkach zmieniającego się środowiska międzynarodowego? W pierwszej części rozdziału wyjaśniono teoretyczne podstawy bezpieczeństwa państwa, przedstawiając ewolucję pojęć „państwa" i „bezpieczeństwa" oraz ukazując ich ścisły związek z rozwojem myśli filozoficznej i politologicznej. Następnie przeanalizowano miejsce państwa w relacjach międzynarodowych, akcentując wpływ umiędzynarodowienia oraz procesów integracyjnych na odporność i pozycję państw w globalnym układzie sił. Kolejna część pracy została poświęcona geopolityce, która została ukazana jako naukowy paradygmat i praktyczne narzędzie analityczne niezbędne do zrozumienia

Summary

The aim of the chapter is to identify the role that geopolitics plays in shaping the strategies of countries to ensure their security in the face of global threats. The research problem was formulated: what is the importance of geopolitics as a paradigm for state security in the conditions of a changing international environment? The first part of the chapter explains the theoretical foundations of state security, presenting the evolution of the concepts of "state" and "security" and showing their close relationship with the development of philosophical and political thought. Then, the place of the state in international relations was analyzed, emphasizing the impact of internationalization and integration processes on the resilience and position of states in the global balance of power. The next part of the work is devoted to geopolitics, which is shown as a scientific paradigm and a practical analytical tool necessary to understand

współczesnych uwarunkowań bezpieczeństwa. Omówiono również wyzwania i zagrożenia geopolityczne, takie jak konflikty zbrojne, protekcjonizm handlowy, rywalizacja technologiczna oraz cyberataki, które determinują działania państw na arenie międzynarodowej. Głównym wnioskiem płynącym z przeprowadzonych analiz jest stwierdzenie, że geopolityka, traktowana zarówno jako koncepcja badawcza, jak i narzędzie praktyczne, odgrywa kluczową rolę w kształtowaniu polityki bezpieczeństwa państwa, umożliwiając skuteczne identyfikowanie i neutralizowanie zagrożeń w warunkach złożoności współczesnego świata. W rozdziale wykorzystano metody teoretyczne, takie jak analiza literatury przedmiotu oraz metoda analityczno-syntetyczna, co pozwoliło na kompleksowe ujęcie poruszanych zagadnień.

Słowa kluczowe: bezpieczeństwo państwa, stosunki międzynarodowe, geopolityka, zagrożenia geopolityczne

contemporary security conditions. Geopolitical challenges and threats, such as armed conflicts, trade protectionism, technological rivalry and cyberattacks, which determine the actions of states in the international arena, are also discussed. The main conclusion of the analyses is that geopolitics, treated both as a research concept and a practical tool, plays a key role in shaping state security policy, enabling effective identification and neutralization of threats in the conditions of the complexity of the modern world. The chapter uses theoretical methods, such as the analysis of the literature on the subject and the analytical-synthetic method, which allowed for a comprehensive approach to the issues raised.

Keywords: state security, international relations, geopolitics, geopolitical threats

Wstęp

Problematyka bezpieczeństwa znajduje się na szczycie celów realizowanych przez każde państwo. Powyższa kwestia odnosi się do dwojakiego postrzegania sposobów wypracowywania stanu stabilności i zrównoważonego rozwoju państwa. Dlatego też bezpieczeństwo państwa należy pojmować w ujęciu wewnętrznym i zewnętrznym (międzynarodowym), a ta dwojakość związana jest z realizacją potrzeb bezpieczeństwa państwa. Sfera wewnętrzna odnosi się do funkcjonowania państwa jako podmiotu wyposażonego w skuteczny aparat państwowy, który efektywnie przeciwdziała, eliminuje bądź ogranicza zagrożenia dla porządku i ładu społecznego[1]. Bezpieczeństwo wewnętrzne to zagwarantowanie stabilność i harmonijność podmiotu, obejmując wszystko to, co wiąże się z równowagą i ładem tego podmiotu. Uzupełnieniem tego ujęcia jest bezpieczeństwo zewnętrzne państwa ujmowane

[1] K. Świerszcz, *Bezpieczeństwo państwa w czasach współczesnych w ujęciu podmiotowo-aksjologicznych wyzwań*, Wydział Logistyki WAT, Instytut Systemów Bezpieczeństwa i Obronności, Warszawa 2016, s. 68-69.

jako brak zagrożeń ze strony innych podmiotów stosunków międzynarodowych. Wiąże się je bezpośrednio z ochroną i obroną przeciwko agresji, a źródeł takich zagrożeń należy upatrywać w otoczeniu państwa. Uzasadnieniem takiego podejścia jest zmienność środowiska bezpieczeństwa i ujmowanie jego w złożony proces, dotyczący ogółu wszystkich czynników otoczenia podmiotu bezpieczeństwa oraz jako wyzwania, szanse, zagrożenia i ryzyka związane z istnieniem państwa. By skuteczne przeciwdziałać współczesnym zagrożeniom niezbędne jest całościowe podejście do bezpieczeństwa zarówno w skali lokalnej, narodowej, jaki i międzynarodowej[2]. Z tychże powodów bezpieczeństwo państwa odnoszone jest do międzynarodowego podmiotu, jakim jest państwo, które prowadzi politykę zagraniczną oraz politykę bezpieczeństwa w zakresie nawiązywania relacji i stosunków międzynarodowych, realizując własne interesy. Uzasadnieniem dla tej tezy jest to, że oznacza zarówno zdolność i gwarancję jego niepodległego oraz suwerennego funkcjonowania, jak i przesłanki rozwoju, spełniania uznanych wartości i aspiracji ogółu narodu w zakresie zapewnienia dobrobytu społecznego, możliwości utrwalenia i przekazywania następnym pokoleniom swojej spuścizny i dziedzictwa. Obejmuje newralgiczne z punktu widzenia postępu ludzkiego dziedziny tj.: ekonomiczną, społeczną, polityczną, technologiczną i kulturową[3]. Toteż współczesne bezpieczeństwo państwa należy traktować nie tylko przez pryzmat militarny, ale także w odniesieniu do poszerzonych płaszczyzn odnoszących się do powyższych obszarów. Problematyka dziedzin kreujących bezpieczeństwo państwa odgrywa znamienną rolę w rywalizacji między narodami, ponieważ na tych polach realizowane są potrzeby państwa i jego społeczeństwa[4].

Teoretyczne aspekty bezpieczeństwa państwa

Problematyka bezpieczeństwa państwa dotyczy wieloaspektowych dylematów. Zagadnienie to posiada złożony charakter, toteż dyskusję warto rozpocząć od wyjaśnienia dwóch podstawowych pojęć, tj. państwa i bezpieczeństwa. Na wstępie rozważań w zakresie definiowania pierwszego terminu,

[2] B. Zdrodowski, *Istota bezpieczeństwa państwa*, Annales Universitatis Paedagogicae Cracoviensis, Studia de Securitate, 9(3), 2019, s. 52-53, 55.

[3] E. Zalewska, *Ryzyka globalizacyjne we współczesnym świecie i ich wpływ na przedsiębiorstwa globalne*, Civitas Hominibus nr 21, Prace studenckie. Politechnika Łódzka 2021, s 143.

[4] J. Płaczek, *Wymiary bezpieczeństwa narodowego – zarys teorii,* Lotnicza Akademia Wojskowa, Dęblin 2022, s. 12.

należy przedstawić poglądy filozofów, którzy poświęcili wiele uwagi zagadnieniu dotyczącemu idei istnienia państwa. Bez wątpienia zainteresowanie pojęciem państwa sięga początków nauk geograficznych i początków nauki w ogóle. Stały się one domeną prac geografów politycznych, a ich analizy dotyczyły różnych poziomów – makro, mezo i mikro, gdzie zawsze punktem odniesienia było państwo, jako podstawowy byt polityczny szeroko rozumianych narodów. Konstytutywne i metodyczne badania kwestii istnienia państwa pochodzą z okresu z V w. p.n.e. i czasów miast-państw. Jednym z pierwszych uczonych, który podjął się próby określenia znaczenia państwa był Platon. Twierdził on, że państwo tworzy się dlatego, że żaden człowiek nie jest i nigdy będzie samowystarczalny[5]. Uznał, że potrzeba przynależności do danej zbiorowości podyktowana jest wzajemnym wsparciem i przeżyciem. Uważał państwo za organizm społeczny dający możliwość zharmonizowania działania klas ludzkich w jedną całość. Filozof ten zdefiniował państwo poprzez określenie – rozrastania struktury społecznej, która zechce być jednością w danych granicach. Swój wkład w tworzenie pojęcia państwa miał uczeń Platona, Arystoteles, który uznał je jako wspólnotę terytorialną i organizację obejmującą zakresem swego działania ogół członków zamieszkujących dane terytorium. Ukazał kwestię prawa i uregulowań prawnych, które miały zapewnić poddanym sprawiedliwość i byt. Od tego filozofa wywodzi się koncepcja traktująca państwo, jak efekt naturalnego społecznego instynktu człowieka. Uważał państwo jako wspólnotę różnych grup ludzi, niezbędnych do jego istnienia. Jego zdaniem państwo jako twór natury powinno całkowicie zaspokajać potrzeby obywateli. Rozważania w tej materii podjął także katolicki uczony Tomasz z Akwinu wskazując, że państwo jako dana społeczność jest doskonałą, samowystarczalną, niezależną oraz samorządową całością. Stosownie do katolickiej nauki społecznej istnienie państwa ściśle związane jest z występowaniem pewnego porządku prawnego oraz władzy, która miała chronić i posiadać możliwości zaspokajania potrzeb obywateli, gwarantując im pokój wewnątrz i na zewnątrz struktury. W dalszym toku rozważań nie sposób nie wskazać założeń pojęcia państwa Georga Jellinka. Myśl tego niemieckiego teoretyka skupiała się na określeniu tego terminu jako korporacji osiadłego ludu, wyposażonego w bezpośrednią samorodną władzę zwierzchnią lub korporację terytorialną wyposażoną w aparat władzy. Przedstawiona

[5] E. Klima, *Państwo – historia idei*, Acta Universitatis Lodziensis, Folia Geographica Socio-Oeconomica 10, Łódź 2009, s. 4-5.

przez tego uczonego definicja państwa stała się podstawą międzynarodowych uregulowań prawnych. Stanowi fundament dla rozróżnienia instytucji państwa od innych organizacji funkcjonujących na arenie międzynarodowej i w globalnym życiu społecznym. Uznanie podmiotowość państwa zobrazowane jest w postanowieniach *Karty Narodów Zjednoczonych,* która wskazuje państwa, jako suwerenne jednostki geopolityczne, stanowiące podmiot wszelakich relacji międzynarodowych. Atrybutami określającymi podmiotowość instytucji państwa są: ludność, określone terytorium, rząd oraz zdolności do utrzymywania relacji z innymi państwami w zakresie realizacji własnych interesów narodowych[6]. Innym wybitnym uczonym był włoski filozof epoki odrodzenia Niccolo Machiavelli, który uważał, że państwo powinno mieć ustrój republikański i stać na straży porządku społecznego, zapewniającego człowiekowi obdarzonemu energią właściwe pokierowanie swoją wolą i działaniem[7]. Mając na uwadze dorobek historyczny i naukowy w tej materii oraz rozwój cywilizacyjny, należy również pochylić się na współczesnym wymiarem rozumienia pojęcia państwa, które zawarte jest w licznych opracowaniach naukowych i leksykalnych. Według definicji politologicznej państwo określa się jako przymusową organizację, zaopatrzoną w atrybuty władzy zwierzchniej. Zasadniczym celem jego funkcjonowania jest ochrona przed zagrożeniami zewnętrznymi i wewnętrznymi oraz zagwarantowanie społeczności zasiedlającej dane terytorium sprzyjających warunków do egzystencji, rozwoju oraz sposobności życia w rzeczywistości ładu i porządku[8].

Z kolei Andrew Heywood, politolog brytyjski stwierdza, że państwo tworzy szczególnego rodzaju stowarzyszenie polityczne. Jego misją jest ustanowienie niezależnej jurysdykcji oraz nieograniczonej władzy w obrębie określonych granic terytorialnych[9]. Z państwem wiążą się pojęcia takie jak: obywatelstwo, suwerenność, władza, naród, społeczeństwo, granice, terytorium. Powyższe atrybuty dają człowiekowi prawo do obywatelstwa, to jedno z podstawowych praw jednostki. Wraz z rozwojem nowoczesnych społeczeństw pojawił się system wartości i praw człowieka. Toteż obecne państwa ustalają

[6] A. Urbanek, red. nauk., *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, Wydawnictwo Społeczno-Prawne, Słupsk 2013, s. 13.

[7] B. Wiśniewski, *Systemy bezpieczeństwa państwa. Konteksty teoretyczne i praktyczne*, Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie, Szczytno 2013, s. 24-26.

[8] M. Gulczyński, *Nauka o polityce*, AlmaMer, Wyższa Szkoła Ekonomiczna, Warszawa 2007, s. 107-109.

[9] A. Heywood, *Teoria polityki. Wprowadzenie*, tłum. Jasiński M., Maliszewska B., Stasiak D., Wydawnictwo Naukowe PWN, Warszawa 2009, s. 80.

swoje cele w oparciu o fundamentalne wartości bytu, przetrwania i rozwoju struktury społecznej. Jednym z elementarnych postulatów państwa jest zapewnienie bezpieczeństwa, które jest efektem uniwersalnego prawa do przeżycia i poczucia bezpieczeństwa, co oznacza niezależność oraz wyłączność aparatu państwowego na zastosowanie odpowiednich sił i środków[10]. Współcześnie bezpieczeństwo państwa jest powszechnie i szeroko używanym terminem w kontekście wielu aspektów działania państwa, co można zauważyć w wypowiedziach uczonych lub w szerokiej debacie społecznej bądź politycznej, a także w licznych przekazach medialnych.

Etymologiczna geneza terminu bezpieczeństwo pochodzi z języka łacińskiego, w którym jest określane ono mianem *securitas,* gdzie *sine* oznacza „bez", zaś *cura* to „*obawa*". W takim wypadku będziemy rozumieli je jako brak obaw, czy też zagrożeń[11]. Warto zwrócić uwagę na inną interpretację, którą zaproponował F. Kaufmann. Mianowicie istnienie danego podmiotu *bez pieczy* nad otaczającymi go zjawiskami niosącymi zagrożenia, które w sferze świadomości podmiotu (naród, grupa społeczna, jednostka) są niepożądane, ze względu na ich negatywne skutki. Autor sugeruje, że pojawienie się zagrożenia było pierwotne wobec ustanowienia pewnego poziomu bezpieczeństwa, a więc wymagało odpowiednich działań[12].

Bezpieczeństwo to jedna z najwyżej cenionych wartości przez każdego człowieka, która jest jednocześnie jedną z jego pierwotnych potrzeb. Bezpieczeństwo należy uznać za niezwykle istotną wartość, potrzebę jednostki oraz narodową. To fundament budowania sprawnie funkcjonującego państwa, które aktywnie zabiega o przetrwanie tożsamości narodowej i tworzy stabilne warunki bytowe dla obecnych i przyszłych pokoleń[13]. Zagwarantowanie bezpieczeństwa ustanowione jest w prawie konstytucyjnym, które stanowi najważniejszy wymiar w procesie kształtowania bezpieczeństwa. Konkretyzuje podstawowe przywileje i wolności obywatela oraz możliwości rozwojowe, co w pełni odzwierciedla bytowe potrzeby i wartości państwa. Bezpieczeństwo należy uznać za jedną z podstawowych potrzeb podmiotowych mającą charakter egzystencjonalny i rozwojowy a osiągnięcie tej potrzeb i wypracowanie

[10] B. Wiśniewski*, Systemy bezpieczeństwa* …, op. cit., s. 33.

[11] J. Kaczmarek, A. Skowroński, *Bezpieczeństwo: Świat – Europa – Polska*, Wrocław 1998, s. 5.

[12] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje – struktury – funkcjonowanie*, wyd. 4, Warszawa 2004, s. 28.

[13] R. Jakubczak, A. Skrabacz, K. Gąsiorek, red. nauk, *Obrona narodowa w tworzeniu bezpieczeństwa Polski w XXI wieku*, Bellona, Warszawa 2008, s. 11.

zamierzonego stanu bezpieczeństwa w państwie uwarunkowane jest istnieniem podstawowych wartości, do których zaliczamy:

- przetrwanie państwa w postaci autonomicznej jednostki politycznej, narodu jako wyodrębnionej grupy etnicznej oraz biologicznego przeżycia ludności;
- integralność terytorialną;
- niezależność polityczną (suwerenność);
- jakość życia wynikającą z możliwości samorealizacji oraz osiągnięcia korzystnych standardów życia, szczebla rozwoju społeczno-gospodarczego, zakresu praw i swobód obywatelskich, dostępu do rozwiniętego systemu społeczno-kulturowego[14].

Kwestie związane z zapewnieniem bezpieczeństwa pełnią nadrzędną rolę, ponieważ świadczą o prawidłowym funkcjonowaniu państwa w skali regionalnej i globalnej. Generalizując, bezpieczeństwo państwa należy traktować jako umiejętność zabezpieczenia integralnych wartości danego państwa przed zewnętrznymi i wewnętrznymi zagrożeniami[15].

Umiejscowienie państwa w relacjach międzynarodowych – ich specyfika oraz implikacje w obliczu współczesnych wyzwań i zagrożeń

Spojrzenie na bezpieczeństwo państwa przez pryzmat relacji światowych i skuteczności wypełniania interesów narodowych powinno obejmować i łączyć funkcjonujące oddzielnie dociekania oraz analizy związane z pozycją państwa na arenie międzynarodowej i jego odpornością na współczesne zagrożenia. Aktualna aktywność podmiotów skupiona jest głównie na elementach dbałości o poziom bezpieczeństwa oraz ochronę przed zagrożeniami dla uznawanych wewnętrznie wartości. W przypadku każdego państwa w zależności od stopnia jego rozwoju, mogą wystąpić różnorodne turbulencje i zagrożenia, które w miarę pojawiania się mogą spowodować zmiany podstawowych wartości u obywateli i w organizacjach funkcjonujących w ramach struktur państwowych. Modelowanie przestrzeni bezpieczeństwa państwa w obecnych czasach nabiera szczególnego znaczenia, ponieważ w latach dziewięćdziesiątych ubiegłego wieku ukazały się z dużą wyrazistością nowe zjawiska

[14] R. Zięba, *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwo Akademickie i Profesjonalne Sp. z o.o., Warszawa 2008, s. 15.

[15] K. Grosicka, L. Grosicki, P. Grosicki, *Organizacja i kierowanie instytucjami bezpieczeństwa wewnętrznego państwa*, Wydawca Aspra, Warszawa 2013, s. 18-19.

determinujące ewolucję bezpieczeństwa w środowisku międzynarodowym. Na uwagę zasługuje zjawisko umiędzynarodowienia bytu narodów i państw, które skutkuje wzrostem korelacji we wszystkich dziedzinach stosunków międzynarodowych, w tym również w sferze bezpieczeństwa. Postęp cywilizacyjny, trendy światowe, rozwój nowoczesnych technologii wyznaczają tempo i kierunek zmian, stanowiąc jednocześnie potencjalne źródło zagrożeń, co czyni je wyzwaniem dla współczesnych dziedzin bezpieczeństwa państwa. W dyskursie i polemikach naukowych obecnie duże znaczenie przywiązuje się do paradygmatu geopolitycznego, jako ważnego czynnika bezpieczeństwa państwa. Zaznaczyć należy, że tak długo, jak państwo utrzymywać będzie dominującą rolę w stosunkach międzynarodowych, tak znaczenie czynnika geopolitycznego, związku potencjału i siły państwa oraz skali geograficznego oddziaływania, będzie miało znaczące miejsce w analizach bezpieczeństwa[16]. Uznać należy, że umiejętny wybór roli międzynarodowej państwa pozwala budować korzystną pozycje międzynarodową i utrzymywać korzystne funkcje w systemie bezpieczeństwa międzynarodowego, co daje możliwość wypracowania wyższego poziomu bezpieczeństwa[17]. Aby państwo mogło osiągnąć określony stopień bezpieczeństwa podejmuje szereg różnorodnych działań. Uzasadniając to stwierdzenie należy wskazać, że najważniejszą formą prac na rzecz szeroko pojętego bezpieczeństwa jest realizacja założeń i dążeń polityki bezpieczeństwa i polityki zagranicznej. Polityka bezpieczeństwa to celowe i zamierzone działania decyzyjne wyspecjalizowanych instytucji państwa ukierunkowane na tworzenie, utrzymanie oraz rozwój systemów bezpieczeństwa o charakterze militarnym i niemilitarnym. To reakcja państwa na aktualne i perspektywiczne zagrożenia oraz wyzwania, jakie mogą urzeczywistnić się w otoczeniu bliższym i dalszym państwa. Polityka bezpieczeństwa jest domeną publiczną, czyli ukierunkowanym procesem oddziaływania władz publicznych w celu rozwiązywania problemów środowiska bezpieczeństwa, w wymiarze regionalnym i globalnym[18]. Główną przesłanką oraz podstawą wyznaczenia i ustalenia dążeń oraz zadań w zakresie polityki bezpieczeństwa jest ustawa zasadnicza, Konstytucja RP, art. 5, która stwierdza, że „Rzeczypospolita Polska strzeże

[16] M. Badak, *Bezpieczeństwo w aspekcie interesów ekonomicznych państwa,* Przegląd Bezpieczeństwa Wewnętrznego, nr 3, 2010, s. 140-142.

[17] T. Pawłuszko, *Polityka bezpieczeństwa Polski – wnioski z badań empirycznych. Polityka bezpieczeństwa Polski – wnioski z badań empirycznych*, Przegląd Geopolityczny nr 43, 2023, s. 52.

[18] Ibidem, s. 49.

niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwa obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju". Powyższy zapis nakłada na organy państwa obowiązek zapewnienia bezpieczeństwa uznając go za podstawowy cel, który realizowany jest w ramach działań sceny politycznej, w zakresie, między innymi, polityki zagranicznej. Realizacja dążeń w tym wymiarze determinowana jest czynnikami wewnętrznymi i zewnętrznymi, które pozwalają osiągnąć korzystną pozycję państwa na arenie międzynarodowej poprzez mobilizację posiadanych zasobów oraz sił i środków[19]. Obecnie należy mieć pełną świadomość, że ważnym elementem starań podejmowanych w zakresie zagwarantowania bezpieczeństwa państwa jest polityka zagraniczna, która stanowi pewnego rodzaju fundament tych działań. Ukierunkowane są one suwerenną aktywnością kompetentnych organów państwa na skuteczną realizację celów strategicznych i interesów mających wymiar narodowy, na arenie międzynarodowej, w bliskiej i dalekiej perspektywie. Dodając, że dążenia w tej kwestii podejmowane są zwłaszcza przez dyplomację i jej skuteczne oddziaływanie na środowisko międzynarodowe. Sfera ta służy przede wszystkim zagwarantowaniu bezpieczeństwa zewnętrznego państwa i dobrobytu narodu, skutecznej obronie interesów narodowych na płaszczyźnie relacji międzynarodowych. Koncepcją polityki zagranicznej jest działalność podmiotów politycznych ukierunkowanych na działalność zewnętrzną państwową w imię racji stanu, a podstawową ideologią jest regulowanie i rozwijanie stosunków z innymi państwami i uczestnikami stosunków międzynarodowych, wyłączając organizacje międzynarodowe i ugrupowania integracyjne[20]. We współczesnym świecie polityka jest zjawiskiem wielowymiarowym. Możemy zatem mówić o polityce w wymiarze globalnym, regionalnym, narodowym czy wewnętrznym. Polityka globalna obejmuje kwestie dotyczące wszystkich państw, to jest w skali całego globu i przyjmuje się, że jest realizowana głównie przez kraje

[19] T. Goryca, *Polityka i strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej – wstęp do dyskusji*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy, nr 41(4), 2021, s. 45.

[20] K. Jaworski, *Teoretyczne aspekty analizy polityki zagranicznej państwa*, Myśl ekonomiczna i polityczna, 30(3), 2010, s. 139-181.

najsilniejsze, które w tejże skali są w stanie zadbać o swoje szeroko pojmowane interesy związane z bezpieczeństwem w każdym jego wymiarze[21].

Relacje uczestników stosunków międzynarodowych, jakie modelują się w światowych trendach kształtujących poziom bezpieczeństwa oraz realizację narodowych interesów odznaczają się dużą złożonością i dynamiką. Są one również zdominowane przez napięcia, sytuacje kryzysowe bądź konflikty, a niektóre państwa realizują swoje interesy za pomocą polityki siły. Obecnie nie bez znaczenia w tych stosunkach ma wpływ dominujący charakter państwa w stosunkach światowych. W tym obszarze występuje różnorodność determinant wewnętrznych i zewnętrznych czynników, które wpływają na dobór właściwych elementów i narzędzi budujących odpowiednią pozycję państwa na arenie międzynarodowej. Międzynarodowe stosunki pojmowane są jako pewnego rodzaju odmiana stosunków międzyludzkich o zróżnicowanych formach współpracy, rywalizacji bądź walki. Formy te oddziałują w dużym stopniu na dobór najskuteczniejszych instrumentów realizacji celów i interesów państwowych. Uznanie jednej z powyżej wskazanych form za dominującą, przy realizacji celów państwowych na arenie międzynarodowej, determinuje najefektywniejsze metody i środki ich urzeczywistnienia. Uwarunkowania te mają duże znaczenie dla oceny ważności oraz przydatności poszczególnych zasobów materialnych i niematerialnych, pozostających w dyspozycji państwa. Rozpatrując relacje na arenie międzynarodowej w kategorii współpracy, należy stwierdzić, że ta forma będzie skutkować odbieraniem innych uczestników stosunków międzynarodowych jako partnerów, współpracowników bądź wspólników, a także jako wrogów i przeciwników. W tych relacjach mogą wystąpić sytuacje sporne, kryzysy bądź konflikty o heterogenicznym podłożu. Mając na uwadze niekorzystne zjawiska bądź okoliczności, uczestnicy tych relacji powinni traktować te uwarunkowania jako wspólny problem do rozwiązania, gdzie celem jest zapewnienie, w jak największym stopniu realizacji interesów wszystkich stron uznając, że każda z nich powinna i może odnieść oczekiwane korzyści. Ponadto powinno się poszukiwać elastycznych i kreatywnych narzędzi rozwiązania problemów. Relacje pomiędzy podmiotami stosunków międzynarodowych postrzegane są w perspektywie długookresowej. W wieloletnich relacjach na arenie międzynarodowej istotnymi priorytetowymi zasobami będą jakość dyplomacji, sojusze oraz układy współpracy

[21] B. Hołyst, *Bezpieczeństwo. Ogólne problemy badawcze,* Wydawnictwo Naukowe PWN, Warszawa 2014, s. 224.

i integracji, a także poziom rozwoju gospodarczo-technicznego. Kolejną formą relacji na arenie międzynarodowej jest walka, gdzie drugą stronę określamy jako wroga, któremu nie można ufać w relacjach. W tej formie relacji można stosować różnorodne narzędzia ograniczające stosunki międzynarodowe pomiędzy wrogimi uczestnikami. Zaś odnosząc się do relacji w stosunkach międzynarodowych jako rywalizacji lub współzawodnictwie, stawia w centrum uwagi obiektywny interes państwa. Nadrzędnym celem jest zapewnienie jak najpełniejszej realizacji założeń i planów, także kosztem innych uczestników relacji międzynarodowych. W stosunkach tych strona przeciwna określana jest jako rywal, konkurent, z którym należy współzawodniczyć. Współzależności w stosunkach międzynarodowych są niewątpliwie zespołem wszystkich trzech podstawowych form – współpracy, rywalizacji i walki, a ich wzajemny stosunek ulega nieustannym dynamicznym zmianom[22]. Reasumując powyższe rozważania należy stwierdzić, że „życie międzynarodowe jest syntezą współpracy i walki w różnych dziedzinach i różnych proporcjach"[23].

Paradygmat geopolityki a współczesny wymiar bezpieczeństwa państwa

Określając rolę i miejsce przestrzeni w działalności i funkcjonowaniu państwa, trzeba wskazać istotne z punktu widzenia analiz politologicznych znaczenie geografii, jako wiedzy o przestrzeni. Dziedzina ta jest istotną determinantą postaw, relacji, zachowań i aktywności politycznych ludzi, a także czynnikiem kształtującym bezpieczeństwo państwa i obywateli.

Wiedza o związkach pomiędzy działalnością polityczną człowieka a przestrzenią geograficzną, która go otacza, stanowi ważny element działań światopoglądowych, w których stara się ukazać wpływ, jaki wywiera na rozwój państwa i jego otoczenie fizyczne. Daje wskazówki, jak zapobiegać zagrożeniom i wykorzystywać zdolności oraz szanse generowane przez położenie. W dobie kształtowania się nowożytnej nauki, wiedza ta zaczęła uzyskiwać stopniową autonomię, toteż zaczęto określać ją jako geografię polityczną lub

[22] M. Kleinowski, *Czynniki budujące siłę i potęgę państwa na arenie międzynarodowej*, Świat idei i polityki, Rocznik Instytutu Nauk Politycznych Uniwersytetu Kazimierza Wielkiego w Bydgoszczy, Tom 10, Wydawnictwo Adam Marszałek, Toruń 2010, s. 11-14.

[23] M. Sułek, *Badania i pomiar potęgi państw – próba odpowiedzi na informacyjne potrzeby decydentów*, [w:] *Stosunki międzynarodowe w XXI wieku, Księga jubileuszowa okazji 30-lecia Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego*, red. nauk. E. Haliżak, R. Kuźniar, G. Michałowska, S. Parzymies, J. Symonides, R. Zięba, Wydawnictwo Naukowe Scholar Warszawa 2006, s. 283.

geopolitykę. Podejmując się rozważań w zakresie pojęcia geopolityki należy uznać, że to termin o wieloaspektowym znaczeniu i szczegółowej sferze problematyki. Prekursorem i projektodawcą tej kategorii był szwedzki uczony Rudolf Kjellen, który w 1899 r. po raz pierwszy użył terminu „geopolityka" w swych dociekaniach. Twórca tego terminu pisał, iż jest to nauka o państwie jako o organizmie geograficznym lub zjawisku przestrzennym. Zauważył, że to wiedza o ziemi i terytorium, a także o wnikliwych terytorialnych formach władzy. Zwraca swoistą uwagę, iż zagadnienie to rozpatrywane jest w dwóch fundamentalnych znaczeniach, tj.:

- Po pierwsze na poszukiwaniu określenia badań w zakresie relacji i związku między szeroko rozumianym środowiskiem geograficznym a polityką.
- Po drugie na sformułowaniu doktryny politycznej eksponującej znaczenie czynników geograficznych w rozwoju stosunków politycznych.

Geopolityka to dziedzina wiedzy traktowana jako paradygmat, współcześnie oznacza określony wzorzec, model, zbiór, metody oraz matrycę badania określonych problemów bezpieczeństwa w zakresie stosunków międzynarodowych. Geopolityka uznawana jest jako teoria w ramach paradygmatu neorealistycznych relacji światowych. Dodać należy, że jest poglądem na świat, teorią lub grupą teorii mających wspólną wizję świata oraz wspólny przedmiot badań, ustalając określone kryteria[24]. W bieżących badaniach przestrzennego uwarunkowania procesów politycznych tradycyjne oraz nowe pola badawcze uzupełniają się, podejmując problemy istotne dla analizy zjawisk i kwestii politycznych. W zakresie prowadzonych prac analitycznych na styku politologii i geografii szczególnie istotne oraz znamienne w ostatnim czasie stały się zagadnienia dotyczące konfliktów regionalnych, przestrzennych, problemów granic, polityki ekologicznej i sporów o surowce, geopolityki, globalizacji nowego ładu międzynarodowego, a także nowych ruchów i działań społecznych[25].

Zarówno problemy usytuowania geograficznego, jak i procesy polityczne to zjawiska dynamiczne, które wzajemnie na siebie oddziaływują, a geopolityka stara się opisać i wyjaśnić naturę tychże interakcji. Kwestie położenia geograficznego, jak i zachowania na arenie politycznej wykazują szybkozmienny charakter. Uwarunkowania te wykazują zależności względem

[24] L. Sykulski, *Geopolityka, Skrypt dla początkujących*, Seria wydawnicza Skrypty naukowe – Geopolityka XXI, Częstochowa 2014, s.23.

[25] J. Potulski, *Wprowadzenie do geopolityki*, Wydawnictwo Uniwersytet Gdański, Gdańsk 2010, s. 34-35.

siebie poprzez różnego typu oddziaływania, a geopolityka stara się identyfikować zjawiska w tej materii. To dyscyplina naukowa ukształtowana na początku XX w. na pograniczu geografii i politologii, jednakże jej zakres tematyczny nie został do dziś w pełni sprecyzowany. Obecnie geopolityka stała się jedną z najbardziej dynamicznych doktryn i rozwijających się dziedzin badawczych. Jej aktualny charakter przyciąga coraz większą uwagę badaczy i uczonych co powoduje, że staje się ważną kwestią w zakresie kształtowania relacji międzynarodowych, które oddziaływują na bezpieczeństwa państw. We współczesnych badaniach nad środowiskiem międzynarodowym zyskuje coraz większej popularności, a podejście geopolityczne jest kluczowe dla realizacji interesów narodowych.

Dokonując określenia tego zagadnienia, należy stwierdzić, że termin ten nie odnosi się jedynie do rdzenia etymologicznego, mającego pochodzenie w języku greckim od słów „*geo"*, czyli ziemia oraz „*politikos"*, znaczy obywatelski. W starożytnej Grecji geopolityka oznaczała, pewien sposób realizacji celów wewnętrznych i zewnętrznych państwa. Odnosząc się do tego ustalenia, to sens geopolityki wiąże się z dwoma składnikami, z których pierwszy dotyczy uwarunkowań geografii, czyli wpływu czynników geograficznych, w szerokim tego słowa znaczeniu, na politykę państwa. Zasadniczo wśród elementów geograficznych uważano, iż szczególnie duży wpływ na płaszczyznę polityki wywierają określone czynniki, które przedstawia rysunek.



terytorium	położenie geograficzne	specyfika granic	liczba i charakter rzek
położenie, klimat	gleby	surowce naturalne	ludność – liczebność, struktura

Rysunek 1. Czynniki wpływające na politykę
Źródło: J. Potulski, *Wprowadzenie do geopolityki*, Wydawnictwo Uniwersytet Gdański. Gdańsk 2010.

Drugi komponent oznacza realizację polityki państwa wewnątrz kraju i w stosunkach między państwami. Uosabia walkę o władzę, o przestrzeń terytorialną, o zasoby naturalne, o kontrolę nad szlakami transportowymi[26]. Materia ta może być interpretowana jako dyscyplina naukowa, paradygmat

[26] Ibidem, s. 13.

badawczy oraz doktryna polityczna. Znajduje swoje miejsce jako paradygmat poznawczy w aspekcie bezpieczeństwa oraz polityki, jest w ciągłym centrum zainteresowań władz politycznych oraz badaczy bezpieczeństwa. Głównymi wyróżnikami tej kategorii jest naród i przestrzeń, ale współcześnie w badaniach geopolitycznych uwzględnia się parametry współistniejące z elementarnymi atrybutami, takimi jak:

- czas – w odniesieniu do wyznaczonej część, w której dochodzi do zmiany w danej przestrzeni geograficznej;
- proces – dotyczy epizodów historycznych oraz problematyczności powstałych zmian;
- asymetria – rozkład układu sił na arenie międzynarodowej;
- zasoby i bogactwa naturalne – jako czynniki gospodarcze uwzględniane w kreowaniu bezpieczeństwa i polityki zagranicznej państwa;
- typ uprawianej polityki – w zakresie imperatywności władz rządzących;
- uwarunkowania społeczno-kulturowe – potencjał relacji międzyludzkich, w tym międzyrządowych, w odniesieniu do korzyści, jakie te relacje mogą generować dla społeczeństwa w danej przestrzeni geograficznej;
- technologia – jako fundamentalna metoda najefektywniejszego dostępu i przekazu informacji.

Neorealistyczne ujęcie posiada aktualny wymiar co określa, że bezpieczeństwo państwa wynika z jego pozycji międzynarodowej. Pozycja ta warunkowana jest szeregiem parametrów wymiernych, do których zalicza się lokalizację, terytorium, dostępność zasobów materialnych, surowców oraz warunki demograficzne. Czynniki niewymierne to niematerialne parametry odnoszące się do morale narodowego, wizerunku, idei, norm i wartości oraz wiedzy. Zaopatrzenie państwa w ten rodzaj identyfikatorów zwiększa możliwości rozwojowe potencjału militarnego i niemilitarnego. Im większy potencjał polityczny, gospodarczy oraz militarny, tym zwykle wyższym poziom bezpieczeństwa[27]. Uznać należy, że geoprzestrzeń pod kątem badań bezpieczeństwa jest fundamentem do podjęcia racjonalnych działań wspierających i kreujących stan bezpieczeństwa państwa.

[27] T. Pawłuszko, *Polityka bezpieczeństwa Polski – wnioski …*, op. cit., s. 47. Ibidem, s. 49.

Wyzwania, ryzyka i zagrożenia geopolityczne

Zmiany na arenie międzynarodowej powodują, że wyzwania i problemy bezpieczeństwa na stałe goszczą w debatach politycznych. Obecne światowe środowisko bezpieczeństwa nacechowane jest niepewnością, która potęgowana jest przez nie zawsze roztropne postępowanie człowieka, które ostatecznie jest jakąś wypadkową dobrej albo złej woli bądź aktywności jednostek, społeczności i społeczeństw. Przyszłość i stan bezpieczeństwa muszą budzić zastanowienie, ponieważ ostatnie pół wieku dostarczyło wielu dowodów na to, że poczucie bezpieczeństwa niektórych regionów oraz państw zostało poważnie zaburzone[28]. Wyróżniające się negatywne procesy w globalnym środowisku bezpieczeństwa sprawiają, że zagrożenia znajdują się w zainteresowaniu wielu podmiotów sektora państwowego i prywatnego, zarówno ze względów politycznych, gospodarczych, militarnych[29].

Niezaprzeczalnie stan bezpieczeństwa państwa jest odzwierciedleniem postrzegania zjawisk ocenianych jako niebezpieczne lub niekorzystne. Wydaje się, że efektywną minimalizację współczesnych niebezpieczeństw można osiągnąć poprzez współpracę międzynarodową, ale również poprzez rozwój nauki w odniesieniu np. do wymiaru geoprzestrzennego, stanowiący dodatkowy, istotny walor eksploracyjny badań nad bezpieczeństwem - postrzegany w kategoriach nowej jakości poznawczej czy w ujęciu praktycznym w relacjach światowych. Badania w tym obszarze potwierdzają, iż pojęcie bezpieczeństwa nabiera ciągle nowego znaczenia i dotyczy ono zarówno potrzeb człowieka, jak i państw oraz systemów międzynarodowych[30]. W świecie, w którym występują wzajemne powiązania, ale który staje się coraz bardziej nieprzewidywalny, niebezpieczeństwa geopolityczne stanowią ogromny problem dla światowych przywódców, co powoduje, że są oni zmuszeni dostosowywać swoje działania do zmian zachodzących w globalnym środowisku. Zrozumienie zawiłości świata, który jest połączony, ale coraz bardziej podzielony, podkreśla krytyczne znaczenie rozpoznawania i zarządzania ryzykiem geopolitycznym, które powinno być wpisane i aktualizowane na bieżąco w poczynaniach rządów. Aby zrozumieć współczesny krajobraz geopolityczny, działacze sceny

[28] J. Gołębiewski, *Anatomia Bezpieczeństwa*, Wydawnictwo Difin, Warszawa 2015, s. 51.

[29] A. Żebrowski, *Zagrożenia dla bezpieczeństwa państw w XXI wieku (wybrane aspekty)*, Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate 12(1), 2022, s. 9.

[30] A. Łaszczuk, *Bezpieczeństwo geopolityczne – nowy wymiar analiz bezpieczeństwa*, [w:] *Geopolityczne aspekty bezpieczeństwa*, red. nauk. E. Kochanek, K. Ligęza, J. Kupiński, Wydawnictwo Akademickie AMW, 2019, s. 13.

politycznej muszą brać pod uwagę złożoność uwarunkowań podczas podejmowania decyzji politycznych, które oddziałują na relacje światowe. Potrzeba nadążania za zmianami geopolitycznymi powoduje zrozumienie ich implikacji i proaktywne rozwiązywanie wyzwań oraz ograniczanie zagrożeń[31].

W kontekście dociekań ryzyk geopolitycznych za istotne należy uznać zagrożenie ataku kraju wysokorozwiniętego na kraj słabo rozwinięty, który stanowi łatwy cel pod względem braku lub ograniczonego dostępu do technologii, która umożliwia kontakt bojowy na wyrównanym poziomie. Konflikty zbrojne mogę mieć związek z usytuowaniem kraju i dotyczyć aspektów przestrzennych, a także z występowaniem surowców bądź zróżnicowaniem ludności, okoliczności te mogą spowodować upadek państwa. Kolejnym ryzykiem geopolitycznym jest upadek multilateralizmu, który objawia się jako system rozliczeń międzynarodowych, w którym wyrównywanie należności poszczególnych państw jest dokonywane wielostronnie. Jego nieprawidłowe funkcjonowanie bądź rozbieżne zadania współdziałających państw w kwestii identyfikacji problemów, procesów naprawczych i finansowania dóbr i zasobów stanowiących wspólną wartość dodaną. Do ryzyk geopolitycznych należy zaliczyć kryzys ekonomiczny, którego przyczyną mogą być różnorodne turbulencje lub szok gospodarczy, a nawet klęski żywiołowe. Ten rodzaj załamania może spowodować gwałtowne obniżenie popytu czy drastyczne zmiany na rynku walutowym, co może wyrządzić poważne konsekwencji na arenie międzynarodowej.

Obecnie środowisko międzynarodowe stoi w obliczu dramatycznych zmian geopolitycznych. Świat stał się bardziej niestabilny i skomplikowany, wkraczając w nową erę sporów handlowych i ekstremalnych presji. Według raportu Globalny BlackRock Geopolitical Risk Indicator (BGRI) określono ryzyka geopolityczne, które przestawia tabela.

[31] *Top geopolitical risks 2025*, PMG, KPMG Make the Difference, 2025, s. 2.

Tabela 1. Formaty współczesnych ryzyk geopolitycznych

Ryzyko geopolityczne	Szczegóły - opis	Poziom prawdopodobieństwa
Globalny protekcjonizm handlowy	Drastycznie wzrastają cła na towary wwożone do USA, co negatywnie wpływa na perspektywy makroekonomiczne.	Wysoki
Wojna regionalna na Bliskim Wschodzie	Konflikt regionalny przybiera na sile, zagraża infrastrukturze energetycznej i zwiększa niestabilność.	Wysoki
Strategiczna rywalizacja USA-Chiny	Napięcia znacznie rosną w związku z sytuacją na Tajwanie i Morzu Południowochińskim.	Wysoki
Globalne odsprzęganie technologii	Skala i zakres odseparowania technologicznego między USA i Chinami znacznie przyspiesza	Wysoki
Główne ataki cybernetyczne	Ataki cybernetyczne powodują długotrwałe zakłócenia w funkcjonowaniu krytycznej infrastruktury fizycznej i cyfrowej.	Wysoki
Duże ataki terrorystyczne	Atak terrorystyczny powoduje poważne straty w ludziach i zakłócenia w funkcjonowaniu gospodarki.	Wysoki
Konflikt Rosja-NATO	Wojna na Ukrainie przedłuża się, co zwiększa ryzyko eskalacji poza granicami kraju.	Średni
Kryzys polityczny na rynkach wschodzących	Rosnąca fragmentacja globalna stanowi poważne obciążenie dla systemów politycznych i instytucji rynków wschodzących.	Średni
Konflikt w Korei Północnej	Korea Północna kontynuuje rozbudowę swojego potencjału nuklearnego i podejmuje prowokacyjne działania, takie jak wystrzelenie rakiet.	Średni
Fragmentacja europejska	Stłumiony wzrost gospodarczy i ciągła presja inflacyjna w obliczu niestabilnego bezpieczeństwa energetycznego prowadzą do odrodzenia się populizmu.	Niski

Źródło: *Raport Globalny*, BlackRock Geopolitical Risk Indicator (BGRI), 2025 [dostęp: 25.04.2025]

Podsumowanie

Można stwierdzić, że nad obecnymi problemami dotyczącymi zagrożeń pochylają się już nie tylko przywódcy, politycy, stratedzy czy ekonomiści, a całe zastępy analityków reprezentujących różne płaszczyzny i sfery działania człowieka. Badacze uwzględniają wielowymiarowość bezpieczeństwa w swych badaniach, mając na uwadze dobro państwa i jego obywateli w stanie

permanentnego zagrożenia. Toteż krąg badań nad bezpieczeństwem poszerzył się i uwzględnia takie zjawiska jak cyberprzestrzeń, bioterroryzm, kryzys gospodarczy, zmiany klimatyczne, emigracja, zagrożenia symetryczne, zorganizowane grupy przestępcze o charakterze terrorystycznym, skutki postępującej globalizacji, upadłe państwa, epidemie, ekstremizm religijny, konflikty cywilizacyjne. Zakres powyższych niebezpieczeństw określa, że punkt ciężkości obecnych zagrożeń dla państw NATO czy UE przeniósł się z niebezpieczeństw militarnych na niemilitarne i terrorystyczne[32].

Podmioty stosunków międzynarodowych obecnie funkcjonują w sferze dużej zmienności zjawisk a ich środowisko bezpieczeństwa ewoluuje pod wpływem wielu złożonych procesów, tak pozytywnych, jak i negatywnych, mających decydujący wpływ na skalę i dynamikę wyzwań i niebezpieczeństw. To codzienność bogata w złożone zjawiska kształtuje decyzje i działania, zarówno w otoczeniu wewnętrznym, jak i zewnętrznym państwa (państw).

Obecne uwarunkowania i trendy światowe po rozpadzie bipolarnego podziału świata są początkiem jakościowo nowych procesów, które z perspektywy czasu i przemian systemowych, w nowej rzeczywistości mogą budzić wiele poważnych wątpliwości i problemów w skali globalnej i w międzynarodowym środowisku bezpieczeństwa[33].

Literatura

1. Badak M., *Bezpieczeństwo w aspekcie interesów ekonomicznych państwa,* Przegląd Bezpieczeństwa Wewnętrznego, nr 3, 2010, s. 138-146.
2. Gołębiewski J., *Anatomia Bezpieczeństwa*, Wydawnictwo Difin, Warszawa 2015.
3. Goryca T., *Polityka i strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej – wstęp do dyskusji*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy, nr 41(4), 2021, s. 43-55. https://doi.org/10.5604/01.3001.0015.7771.
4. Grosicka K., Grosicki L., Grosicki P., *Organizacja i kierowanie instytucjami bezpieczeństwa wewnętrznego państwa*, Aspra, Warszawa 2013.
5. Gulczyński M., *Nauka o polityce*, AlmaMer Wyższa Szkoła Ekonomiczna, Warszawa 2007.
6. Heywood A., *Teoria polityki Wprowadzenie*, tłum. Jasiński M., Maliszewska B., Stasiak D., Wydawnictwo Naukowe PWN, Warszawa 2009.
7. Hołyst B., Bezpieczeństwo, *Ogólne problemy badawcze*, Wydawnictwo Naukowe PWN 2014.

[32] J. Płaczek, *Wymiary bezpieczeństwa narodowego…*, op. cit., s.13.

[33] A. Żebrowski, *Zagrożenia dla bezpieczeństwa państw w XXI wieku…*, op. cit., s. 9-10.

8. Jakubczak R., Skrabacz A., Gąsiorek K. (red.). *Obrona narodowa w tworzeniu bezpieczeństwa Polski w XXI wieku*, Bellona, Warszawa 2008.
9. Jaworski K., *Teoretyczne aspekty analizy polityki zagranicznej państwa*, Myśl ekonomiczna i polityczna, 30(3), 2010, s. 139-181.
10. Kaczmarek J., Skowroński A., *Bezpieczeństwo: świat – Europa – Polska*, Atla2, Wrocław 1998.
11. Kleinowski M., *Czynniki budujące siłę i potęgę państwa na arenie międzynarodowej*, Świat Idei i Polityki, Rocznik Instytutu Nauk Politycznych Uniwersytetu Kazimierza Wielkiego w Bydgoszczy, Tom 10, Wydawnictwo Adam Marszałek, Toruń 2010, s. 9-36. https://doi.org/10.34767/SIIP.2010.01.01
12. Klima E., *Państwo – historia idei*, Acta Universitatis Lodziensis, Folia Geographica Socio-Oeconomica, nr 10, 2009, s. 3-20.
13. KPMG, *Top geopolitical risks 2025*. Pobrane z: https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2025/03/top-geopolitical-risks-2025-web.pdf#page=1&zoom=auto,-100,546, 2025.
14. Łaszczuk A., *Bezpieczeństwo geopolityczne – nowy wymiar analiz bezpieczeństwa,* [w:] *Geopolityczne aspekty bezpieczeństwa,* red. nauk. E. Kochanek, K. Ligęza, J. Kupiński, Wydawnictwo Akademickie AMW, 2020.
15. Pawłuszko T., *Polityka bezpieczeństwa Polski – wnioski z badań empirycznych. Polityka bezpieczeństwa Polski – wnioski z badań empirycznych*, Przegląd Geopolityczny, 43, 2023, s. 49-70.
16. Płaczek J., Wymiary bezpieczeństwa narodowego – zarys teorii. Lotnicza Akademia Wojskowa. Dęblin 2022.
17. Potulski J., Wprowadzenie do geopolityki. Wydawnictwo Uniwersytet Gdański. Gdańsk 2010.
18. Sułek M., *Badania i pomiar potęgi państw – próba odpowiedzi na informacyjne potrzeby decydentów*, [w:] *Stosunki międzynarodowe w XXI wieku*, Księga jubileuszowa okazji 30-lecia Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego, red. E. Haliżak, R. Kuźniar, G. Michałowska, S. Parzymies, J. Symonides, R. Zięba, Warszawa 2006.
19. Sykulski L., *Geopolityka. Skrypt dla początkujących* Wydawnictwo Naukowe Grategia, Częstochowa 2014.
20. Świerszcz K., *Bezpieczeństwo państwa w czasach współczesnych w ujęciu podmiotowo-aksjologicznych wyzwań*, Przegląd Nauk o Obronności, nr 1-2, 2016, s. 66-82. https://doi.org/10.5604/01.3001.0012.9695
21. Urbanek, A. (red). *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, Wydawnictwo Społeczno – Prawne, Słupsk 2013
22. Wiśniewski, B. *Systemy bezpieczeństwa państwa. Konteksty teoretyczne i praktyczne*. Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie, Szczytno 2013.
23. Zalewska E., *Ryzyka globalizacyjne we współczesnym świecie i ich wpływ na przedsiębiorstwa globalne*, Civitas Hominibus, nr 16, 2021, s. 143-147. https://doi.org/10.25312/2391-5145.16/2021_16ez
24. Zdrodowski B., *Istota bezpieczeństwa państwa*, Annales Universitatis Paedagogicae Cracoviensis, Studia de Securitate, 9(3), 2019, s. 47-71.

25. Zięba R., *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwo Akademickie i Profesjonalne Sp. z o.o. Warszawa 2008.
26. Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje – struktury – funkcjonowanie*, Wydawnictwo Naukowe Scholar, Warszawa 2004.
27. Żebrowski A., *Zagrożenia dla bezpieczeństwa państw w XXI wieku (wybrane aspekty)*, Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate, nr 12(1), 2022, s. 7-31. https://doi.org/10.24917/26578549.12.1.1

dr Anna Opar
Uczelnia Państwowa im. Jana Grodka w Sanoku
ORCID: 0000-0001-9781-178X
https://doi.org/10.29316/9788368103199_2

WSPÓŁCZESNE ZAGROŻENIA BEZPIECZEŃSTWA. TERRORYZM

CONTEMPORARY SECURITY THREATS. TERRORISM

Streszczenie

Według definicji zaproponowanej przez Komisję Europejską terroryzm to „wszelkie celowe akty popełnione przez pojedyncze osoby lub organizacje przeciw jednemu, lub kilku państwom, ich instytucjom lub ludności, w celu zastraszania oraz poważnego osłabienia lub zniszczenia struktury politycznej, gospodarczej i społecznej kraju". W przeszłości zjawisko to miało najczęściej zasięg lokalny bądź regionalny, współcześnie urosło do globalnego problemu. Terroryzm jest jednym z największych zagrożeń współczesnego świata, a poziom zagrożenia terroryzmem może wzrastać. Postęp technologiczny wykorzystywany jako narzędzie, nowe metody i formy działań oraz stosowane środki powodują, że terroryzm staje się zagrożeniem o charakterze ogólnoświatowym. Podmioty odpowiadające za bezpieczeństwo muszą być przygotowane na te zmiany, rozwijać możliwości w zakresie zdobywania informacji, doskonalić procedury reagowania kryzysowego na wypadek ataku terrorystycznego.

Summary

According to the definition proposed by the European Commission, terrorism is "any deliberate act committed by individuals or organizations against one or more States, their institutions or populations, in order to intimidate, seriously weaken or destroy the political, economic and social structure of the country". In the past, this phenomenon was most often local or regional, but today it has grown into a global problem. Terrorism is one of the greatest threats to the modern world, and the level of the threat of terrorism may increase. Technological progress used as a tool, new methods and forms of action and the means used mean that terrorism is becoming a global threat. Entities responsible for security must be prepared for these changes, develop capabilities in the area of obtaining information, and improve crisis response procedures in the event of a terrorist attack. In Poland, according to experts, the level of

W Polsce, zdaniem ekspertów, poziom zagrożenia atakami terrorystycznymi nie jest wysoki, jednak nie można go bagatelizować.

Słowa kluczowe: terroryzm, zagrożenie, bezpieczeństwo

threat from terrorist attacks is not high, but it cannot be underestimated.

Keywords: terrorism, threat, security

Wstęp

Terroryzm jest zjawiskiem złożonym i różnorodnie definiowanym. Cechą specyficzną terroryzmu jest to, że stosowane metody działania są czynami bezprawnymi np. użycie przemocy, branie zakładników czy zamachy bombowe. Przyczyną terroryzmu są kwestie polityczne, ideologiczne, narodowościowe, religijne, społeczne. Na bazie tych czynników powstają ruchy radykalne, nacjonalistyczne czy fundamentalistyczne, które stają się podstawą rozwoju terroryzmu. Dyrektywa unijna w sprawie zwalczanie terroryzmu definiuje terroryzm jako czyny popełnione w celu poważnego zastraszenia ludności, bezprawnego zmuszenia rządu lub organizacji międzynarodowej do podjęcia lub zaniechania jakiegoś działania, poważnej destabilizacji lub zniszczenia podstawowych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych danego państwa lub danej organizacji międzynarodowej[1]. W dobie coraz szybszego rozwoju technologii i postępującej globalizacji, terroryzm zaliczany jest do grupy największych wyzwań i zagrożeń bezpieczeństwa.

Terroryzm, akt terrorystyczny – terminologia

Słownik Języka Polskiego definiuje terror jako „stosowanie przemocy, gwałtu, okrucieństwa w celu zastraszenie, zniszczenia przeciwnika", natomiast terroryzm to „stosowanie terroru dla celów politycznych, zwłaszcza zorganizowana działalność ugrupowań ekstremistycznych (uprowadzenia samolotów, mordowanie polityków, zamachy bombowe itp.), prowadzona dla wywarcia presji na społeczeństwo i władze, wymuszenia ustępstw, korzystnych dla siebie decyzji politycznych"[2]. Znaczenie terminów terror i terroryzm różnią się

[1] *Jak zatrzymać terroryzm: przegląd działań Unii Europejskiej*, https://www.europarl.europa.eu/topics/pl/article/20180316STO99922/jak-zatrzymac-terroryzm-przeglad-dzialan-unii-europejskiej, [dostęp: 02.04.2025].

[2] B. Dunaj (red. nauk.), *Słownik Języka Polskiego*, Wydawnictwo Wilga, Warszawa 2005, s. 710-711.

od siebie w polskiej literaturze przedmiotu. Terror to stosowanie przemocy silniejszych wobec słabszych, natomiast terroryzm rozumiany jest jako przemoc słabszych wobec silniejszych[3].

Alex P. Schmidt, dokonując analizy porównawczej istniejących definicji terroryzmu, stwierdził, że „niemożliwe jest zbudowanie uniwersalnej definicji terroryzmu. Jest to bowiem problem definiowany przede wszystkim w drodze praktyki instytucji międzynarodowych lub organów poszczególnych państw odpowiadających za jego zwalczanie według kryteriów zmiennych w zależności od czasu i zakresu własnej odpowiedzialności. […] można jedynie wyodrębniać wspólne różnym definicjom elementy, pozwalające uchwycić bieżącą istotę nieustannie zmieniającego się zjawiska”[4]. Natomiast samo zjawisko terroryzmu definiuje jako „metodę działania polegającą na stosowaniu wywołujących lęk powtarzalnych aktów przemocy, stosowaną przez utajnione jednostki, grupy lub aktorów państwowych w celach politycznych, gdzie w odróżnieniu od innych form przemocy politycznej, bezpośrednie cele ataków nie są celami głównymi”[5]. Komisja Europejska definiuje terroryzm jako „wszelkie celowe akty popełnione przez pojedyncze osoby lub organizacje przeciw jednemu lub kilku państwom, ich instytucjom lub ludności, w celu zastraszania oraz poważnego osłabienie lub zniszczenia struktury politycznej, gospodarczej lub społecznej kraju”[6].

Wśród polskich badaczy zjawiska funkcjonuje wiele definicji terroryzmu. Według Bartosza Bolechowa: „Terroryzm jest formą przemocy politycznej, polegającej na stosowaniu morderstw lub zniszczenia (albo zagrożeniem stosowania takich środków) w celu wywołania szoku i ekstremalnego zastraszenia jednostek, grup, społeczeństw lub rządów, czego efektem mają być wymuszenia pożądanych ustępstw politycznych, sprowokowanie nieprzemyślanych działań i/lub zademonstrowanie/nagłośnienie politycznych przekonań”[7]. Marek Madej definiuje terroryzm jako „służąca realizacji określonego

[3] T. Wałek, *Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych*, Securitologia 2018, nr 2, s. 112.

[4] K. Kozłowski, *Terroryzm jako zagrożenie państwa*, [w:] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, red. nauk. B. Sulowski, M. Brzeziński, Dom Wydawnictwo Elipsa, Warszawa 2009, s. 300.

[5] R. Cegiełka, *Zagrożenie terroryzmem. Poczucie bezpieczeństwa na początku XXI wieku oraz wpływy terroryzmu na procesy gospodarcze w wymiarach mikro i makro*, Agencja Wydawnicza Synergy Elżbieta Meissner, Warszawa 2015, s. 39

[6] T. Wałek, *Pojęcie, geneza…*, op. cit., s. 115.

[7] B. Bolechów, *Terroryzm w świecie poduwubiegunowym. Przewartościowania i kontynuacje*, Wydawnictwo Adam Marszałek, Toruń 2003, s. 25.

programu politycznego przemoc lub groźba jej użycia ze strony podmiotów niepaństwowych (sub-transnarodowych), która ma wzbudzić strach w grupie szerszej niż bezpośrednio zaatakowani i w ten sposób nakłonić rządy państw do ustępstwa lub doprowadzić do zniszczenia dotychczasowego porządku publicznego”[8]. Według Jerzego Szafrańskiego „terroryzm jest szczegółowym rodzajem działalności destrukcyjnej, skierowanej zarówno przeciwko pojedynczym osobom aparatu władzy (terroryzm indywidualny), również przeciwko przypadkowym członkom społeczeństwa przez zamachy na policjantów, urzędników czy cywili (terroryzm zbiorowy), powodując ofiary oraz wywołując atmosferę strachu. Ofiarami takiej działalności są politycy, wojskowi, policjanci, a także zwykli obywatele, bez względu na płeć, wiek, czy wykształcenie”[9]. Krzysztof Karolczak zdefiniował terroryzm jako: „politycznie umotywowane działanie, które przy użyciu dowolnych metod zastraszających, ma doprowadzić do oczekiwanych zachowań obiektu, wobec którego jest zastosowane”[10]. Marian Flemming tak definiuje pojęcie: „terroryzm to umyślne działania stanowiące naruszenie prawa karnego i zmierzające w drodze aktów przemocy lub zagrożenia takimi aktami do zastraszenia organów państwowych lub znaczących odłamów społeczeństwa oraz do wymuszenia określonego postępowania”[11]. Adam Krawczyk zjawisko terroryzmu określa jako „proces oddziaływania ideologii (światopoglądu) poprzez akty przemocy (lub groźbę ich użycia) zastosowane pośrednio lub bezpośrednio na rozmaite struktury decyzyjne, w celu poddania ich określonemu zachowaniu. Zjawisko to występuje często wraz z innymi czynnikami mającymi na niego bezpośredni lub pośredni wpływ”[12].

Niezależnie od przyjętej definicji pojęcia terroryzm, jest to środek, narzędzie, strategia polityki i jej działanie. Według Roberta Cegiełki terroryzm zawiera […] cztery podstawowe elementy:

- premedytacja - decyzja sprawcy o zamiarze dokonania aktu lub zaszczepienia strachu u innych;

[8] M. Madej, *Międzynarodowy terroryzm polityczny*, Ministerstwo Spraw Zagranicznych, Warszawa 2001, s. 7.

[9] J. Szafrański, *Współdziałanie jednostek obrony terytorialnej i policji w walce z terroryzmem*, Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji, Szczytno 2004, s. 5.

[10] A. Krawczyk, *Wokół definicji terroryzmu*, https://histmag.org/Wokol-definicji-terroryzmu-2399, [dostęp: 31.03.2025].

[11] R. Cegiełka, *Zagrożenie terroryzmem…*, op. cit., s. 33.

[12] A. Krawczyk, Wokół definicji terroryzmu, https://histmag.org/Wokol-definicji-terroryzmu-2399, [dostęp: 31.03.2025].

- motywacja lub sprawa – polityczna, religijna, ekonomiczna;
- cele, przeważnie niewojskowe – np.: osoby ze świata polityki, urzędnicy lub niewinne osoby postronne;
- konspiracja – niezależnie od tego, czy sprawca jest członkiem tajnej organizacji, czy jest w tajemnicy finansowany przez konkretne państwa”[13].

Natomiast zamach terrorystyczny/incydent to „akt przemocy lub wiarygodnego zagrożenia jej użycia (oparty na typowych metodach terrorystycznych), przeprowadzony z pogwałceniem prawa, którego głównym celem jest zastraszenie rządu, społeczeństwa lub jakiejkolwiek jego części, co ma umożliwić realizację założonych celów politycznych”[14]. Według definicji Zgromadzenia Parlamentarnego Rady Europy akt terrorystyczny to „każdy czyn popełniony przez osobę lub grupę osób z udziałem przemocy lub groźby jej użycia przeciwko państwu, jego instytucjom, jego ludności w ogólności lub konkretnym jednostkom, motywowanym przez separatystyczne aspiracje, ekstremistyczne koncepcje ideologiczne, fanatyzm lub irracjonalne i subiektywne czynniki, zorientowany na stworzenie klimatu terroru wśród osób publicznych, określonych jednostek lub grup w społeczeństwie, bądź w całym społeczeństwie”[15]. W polskim systemie prawnym , jedną z ważniejszych ustaw dotyczących terroryzmu jest uchwalona w 2018 roku Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Ustawodawca definiuje akt terrorystyczny jako „przestępstwa przeciwko pokojowi, ludzkości oraz przestępstwa wojenne, przestępstwa przeciwko bezpieczeństwu powszechnemu oraz przestępstwa określone w art. 134 i art. 136. Ustawodawca miał tu na myśli konkretne czyny zabronione zawarte w rozdziałach XVI i XX k.k., penalizujących przestępstwa przeciwko pokojowi, ludzkości i przestępstwa wojenne oraz przestępstwa przeciwko bezpieczeństwu powszechnemu, a także w dwóch wymienionych artykułach tj. w art. 134 (napaść na prezydenta RP) i art. 136 k.k. (napaść na głowę obcego państwa)”[16]. Działania terrorystyczne realizowane są za pomocą różnych środków bezwzględnie, z nadaniem im rozgłosu i celowym wytworzeniem w społeczeństwie lęku.

[13] R. Cegiełka, *Zagrożenia terroryzmem…*, op. cit., s. 36.
[14] B. Bolechów, *Terroryzm w świecie…*, op. cit., s. 25.
[15] T. Wałek, *Pojęcie, geneza…,* op. cit., s. 115.
[16] Ibidem, s. 115.

Historia terroryzmu

Przyjmuje się, że pierwszym terrorystą był Herostrates z Efezu, ubogi szewc, który chcąc zyskać rozgłos w 356 r. p.n.e. podpalił świątynię Artemidy, uważaną przez Greków za jeden z cudów świata[17]. Wybitni greccy filozofowie, Platon czy Arystoteles, rządy tyranów nazywali przestępstwem, bowiem łamali prawa, po władzę sięgali stosując walkę i wykorzystując niezadowolenie pewnych grup. Terroryzm pojawił się w Atenach, gdzie po przegranej wojnie peloponeskiej Spartanie narzucili rządy Ateńczykom, zwane rządami Trzydziestu Tyranów, które pochłonęły życie 1 500 obywateli i spowodowały wygnanie 5 000. W starożytnym Rzymie zabójstwo tyrana uważano za usprawiedliwione, według Seneki dla bogów nie ma milszej ofiary niż krew tyrana, a Cycero pisał: „tyrani zawsze umierali śmiercią gwałtowną, a ich mordercy cieszyli się zazwyczaj sympatią ludu”[18].

Maria Tomczak za pierwszy ruch terrorystyczny uznaje Sicarii, fanatyczną odmianę ugrupowania polityczno-religijnego Zelotów, która działała na terenie Palestyny i Egiptu w pierwszej połowie I w. n. e. Celem sykariuszy, nazywanych tak od ulubionej broni – krótkiego miecza sica, było zniszczenie pałaców dynastii Heroda, spalenie archiwów, utrudnienie dostaw wody do Jerozolimy. Na Bliskim Wschodzie, między XI a XII wiekiem działali asasyni, zorganizowana szyicka sekta specjalizująca się w skrytobójczych zamachach. Ugrupowanie wywodziło się z konserwatywnego odłamu szyitów i jako pierwsze zastosowało zamachy i skrytobójstwo w politycznej walce o władzę[19]. Przykładami państw rządzonych metodami terroru jest Mongolia i Rosja. Teorię uzasadniającą zabójstwo tyrana stworzył w średniowieczy Jan z Salisbury, w XIV wieku rozwinęli ją monarchomachowie[20]. W pierwszej połowie XII wieku Mongołowie stworzyli zmilitaryzowane państwo, rządzone przez Czingis-chana, który dokonując podbojów stosował terror i ludobójstwo na niespotykaną skalę. W Rosji car Iwan Groźny w latach 1564-1572 wprowadził rządy skrajnego terroru tzw. opriczninę. Zbrojne oddziały jeźdźców

[17] R. Borkowski, *Terroryzm*, [w:] *Konflikty współczesnego świata*, red. nauk. R. Borkowski, Wydawnictwo AGH, Kraków 2001, s. 120.

[18] R. Cegiełka, *Zagrożenie terroryzmem…*, op. cit., s. 12; T. Wałek, *Pojęcie, geneza*…, op. cit., s. 116.

[19] R. Cegiełka, *Zagrożenie terroryzmem…*, op. cit., s. 13.

[20] T. Wałek, *Pojęcie, geneza*…, op. cit., s. 116.

w czarnych strojach na czarnych koniach, których godłem była psia głowa i miotła, szerzyły terror grabiąc, mordując i dokonując zesłań bojarów[21].

Terminy terror i terroryzm upowszechniły się w czasie Rewolucji Francuskiej, zwłaszcza w latach 1793-94, w których działalność Komitetu Ocalenia Publicznego i Trybunału Rewolucyjnego nazywano wielkim terrorem. Metodę terroru stosowano wobec każdego podejrzanego o wrogi stosunek do nowej władzy, represje, brutalne i na ogromną skalę, stosowano wobec faktycznych i wyimaginowanych wrogów rewolucji. Ofiary sięgnęły 40 tyś. osób zmarłych i około 300 tyś. represjonowanych, przetrzymywanych w więzieniach. W końcowej fazie terroru jakobinów, najbardziej radykalnego ugrupowania, procesy przed trybunałami rewolucyjnymi prowadzono bez możliwości prawa do obrony oskarżonego, na którym to procesie mógł zapaść wyrok jedynie skazujący na śmierć lub uniewinniający. Krwawych egzekucji i pacyfikacji dokonywano według woli reprezentantów Komitetu, wysłanych na prowincję w celu zaprowadzenia rewolucyjnego porządku, np.: pacyfikacja Lyonu czy tłumienie powstania w Wandei[22].

Nowożytny terroryzm pojawił się w połowie XIX wieku za sprawą anarchistów głoszących hasła buntu przeciwko ówczesnym porządkom społecznym. Anarchiści głosili przekonanie, że zło tkwi w instytucjach politycznych i gospodarczych, stąd ich działalność polegała na walce z przymusem politycznym (państwem), przymusem ekonomicznym (kapitałem), i przymusem moralnym (religią), a celem ostatecznym walki było stworzenie społeczeństwa bez siły i przymusu, bez rządu, w którym równi sobie ludzie osiągną stabilność dzięki porozumieniu pomiędzy różnymi grupami (komunami)[23]. Pod koniec XIX wieku doszło w Europie do serii zamachów terrorystycznych. W roku 1874 we Włoszech odbyło się wiele zamachów terrorystycznych, w tym okresie nastąpiły pierwsze zamachy na głowy państw. W najsłynniejszych zamach terrorystycznych zginęli: prezydent Francji Lazare Hippolyte Carnot w roku 1884, w 1897 roku premier Hiszpanii, José Canalejas de Castillo w 1897, cesarzowa austriacka Elżbieta w roku 1898 i król włoski Humbert w roku 1900, zaś na początku XX wieku prezydent Stanów Zjednoczonych, William McKinley w roku 1901[24]. Po udanym zamachu na cara Aleksandra II w 1881 roku, przeprowadzonego przez ugrupowanie Narodnaja Wola, anarchiści zwołali w Lon-

[21] R. Borkowski, *Terroryzm*, [w:] *Konflikty*…, op. cit., s. 122.

[22] Ibidem, s. 123.

[23] Ibidem.

[24] T. Wałek, *Pojęcie, geneza*…, op. cit., s. 117.

dynie konferencję, na której zaaprobowano zamachy i zabójstwa tyranów jako metodę wprowadzenia rewolucyjnych zmian i utworzono Międzynarodówkę Anarchistyczną, tzw. Czarną Międzynarodówkę[25]. Terroryzm zainspirowany ideologiami nacjonalistycznymi rozwinął się na początku XX wieku, jako terroryzm separatystyczny pojawił się w Irlandii Północnej i na Bałkanach. W 1919 roku powstała Irlandzka Armia Republikańska, której bojownicy nie uznawali traktatu brytyjsko-irlandzkiego, a największe nasilenie działań terrorystycznych przypadło na lata trzydzieste i wiązało się z żądaniem usunięcia, w 1939 roku, wojsk brytyjskich z Irlandii Północnej. Seria eksplozji bombowych, w ciągu kliku miesięcy, zabiła wielu ludzi, w sierpniu tego toku IRA dokonała krwawego zamachu w głównym centrum handlowym w Coventry. Nacjonalistyczne i terrorystyczne organizacje, mające głównie charakter antyhabsburski, zakładali także Serbowie. W 1908 roku powstała organizacja Narodna Obrana, a członkowie jej radykalnej frakcji Czarna Ręka szkolili i wyposażali w broń zamachowców oraz kierowali zamachami w Bośni i Hercegowinie. I wojna światowa wybuchła na skutek zamachu członka organizacji Mlada Bosna, bośniackiego Serba Gavrilo Principa, na arcyksięcia Ferdynanda w Sarajewie w 1914 roku. Terrorystyczny charakter miały działania bojówek faszystowskich w Niemczech - SA, we Włoszech i Hiszpanii – Falanga, w Rumunii – Żelazna Gwardia. W państwach, gdzie partie faszystowskie doszły do władzy, przemoc nabrała charakteru terroru państwowego[26].

Po II wojnie światowej terroryzm odrodził się w latach sześćdziesiątych XX wieku, był wynikiem dekolonizacji, efektem szerzenia się terroryzmu o pochodzeniu lewackim, terroryzmu bliskowschodniego, w tym czasie narodził się również terroryzm międzynarodowy. Ta fala terroryzmu ma swój początek przede wszystkim w Palestynie, gdzie terror stał się metodą rozwiązywania konfliktów między Arabami a Żydami. Za początek terroryzmu międzynarodowego uważany jest rok 1968, gdy Palestyńczycy porwali izraelski samolot w Rzymie. Terroryzm palestyński stał się terroryzmem międzynarodowym, terroryści mogli obrać dowolny cel w dowolnym miejscu świata, np. masakra izraelskich sportowców na igrzyskach olimpijskich w Monachium. Drugim czynnikiem powstania terroryzmu międzynarodowego w latach sześćdziesiątych, była fala rewolucji w krajach Trzeciego Świata oraz tzw. proces dekolonizacji. Kolejnym czynnikiem sprzyjającym były ruchy

[25] R. Borkowski, *Terroryzm*, [w:] *Konflikty*…, op. cit., s. 123.
[26] Ibidem, s. 124-125.

młodego pokolenia na Zachodzie w 1968 roku. Kontestacja sprzyjała szerzeniu się programów radykalnych, lewackich i terrorystycznych. W publicystyce lata siedemdziesiąte zostały nazwane „dekadą ołowiu", były czasem powstania i krwawych zamachów m.in. Czerwonych Brygad we Włoszech, Frakcji Czerwonej Armii w RFN, Tureckiej Armii Wyzwolenia Narodowego. Kraje Europy Zachodniej mierzyły się z terroryzmem separatystycznym organizacji takich jak, m.in.: Irlandzka Armia Republikańska (IRA), baskijska ETA, palestyńskie organizacje – Organizacja Wyzwolenia Palestyny, Ludowy Front Wyzwolenia Palestyny[27].

Rewolucja irańska w 1979 roku, która przekształciła Iran w Republikę Islamską, stała się początkiem terroryzmu islamskiego, motywowanego imperatywem religijnym. Sprawcy legitymizują przemoc traktując ją jako obowiązek lub akt sakramentalny. W 1998 r. w dwu stolicach państw Afryki Wschodniej, Nairobi i Dar es-Saalam, prawie jednocześnie wysadzone zostały w powietrze budynki ambasad Stanów Zjednoczonych. Przy okazji tych zamachów światowa opinia publiczna dowiedziała się o działalności Osamy bin Ladena i Al-Kaidy. Al-Kaida przyznała się również do zamachu w 2000 roku na cumujący w adeńskim (Jemen) porcie niszczyciel USS Cole[28].

Zamach z 11 września 2001 roku, o który oskarżono Al.-Kaidę, na nowojorskie wieże World Trade Center i Pentagon, stał się przełomowy w historii światowego terroryzmu. Do tego czasu był on zjawiskiem międzynarodowym (terroryści z jednego kraju dokonują zamachu na terytorium drugiego w interesie trzeciego), natomiast po 11 września 2001 roku stał się zjawiskiem globalnym ze względu na swój charakter i zasięg. Zamach na WTC był pierwszym zamachem tego typu i pochłonął więcej ofiar i strat, niż jakikolwiek atak terrorystyczny w historii. W Europie w pierwszej dekadzie XXI wieku atakami terrorystycznymi przypisywanymi Al-Kaidzie były zamachy z 11 kwietnia 2004 roku w Madrycie oraz zamachy samobójcze w Londynie z 7 lipca 2005 roku, wymierzone w system transportu publicznego. Po kilku latach przerwy, wraz ze wzrostem w siłę Państwa Islamskiego przetoczyła się przez Europę kolejna fala zamachów.7 stycznia 2015 roku we Francji, w odwecie za zamieszczenie karykatur Mahometa, zaatakowano redakcję satyrycznego czasopisma „Charlie Hebdo", 13 listopada tego samego roku dokonano zamachu w Paryżu, który pod względem jednorazowej liczby ofiar był największym zdarzeniem

[27] Ibidem, s. 125-126.

[28] K. Karolczak, *Terroryzm XXI wieku – wybrane aspekty*, s. 10, https://abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr1/Karolczak_K_.pdf, [dostęp: 03.04.2025].

we Francji od czasów II wojny światowej. W 2016 r. Europą wstrząsnęły kolejne zamachy: 22 marca 2016 roku w Belgii – dwa w porcie lotniczym Bruksela w Zaventem i jeden przy stacji metra Maelbeek w Brukseli, zaś 14 lipca w Nicei[29].

W 2021 r. w państwach członkowskich UE miało miejsce 15 ataków terrorystycznych. Całkowita liczba ataków w 2021 r. była znacznie niższa niż w poprzednich latach. W okresie 2019–2021 w całej UE udaremniono 29 spisków dżihadystycznych lub skrajnie prawicowych[30].

W ostatnich latach wśród ekspertów, coraz częściej pojawiają się obawy przed tzw. superterroryzmem, polegającym na zastosowaniu przez terrorystów broni masowego rażenia lub działań, które mogłyby zdestabilizować sytuację na znacznym obszarze atakowanych państw[31].

Terroryzm – klasyfikacja pojęcia

Klasyfikację działalności terrorystycznej można przeprowadzić w oparciu o różne przyjęte kryteria. Robert Borkowski proponuje następujące kategorie: działający podmiot, cel ataku, taktyka walki, polityczna strategia, założenia doktrynalne i cele ideologiczne.

Ze względu na podmiot dokonujący działań terrorystycznych wyróżnić można: terroryzm polityczny i terroryzm niepolityczny. W obrębie terroryzmu politycznego mieści się terroryzm agenturalny – gdy terroryści są sponsorowani, inspirowani i kierowani przez obce państwo oraz terroryzm ideowy – gdy podstawą działalności terrorystycznej są wyznawane idee. Terroryzm niepolityczny obejmuje terroryzm kryminalny – oznaczający działania mafii i gangów oraz terroryzm szaleńców[32].

Na podstawie celu ataków terrorystycznych wyróżnić można: terroryzm ekonomiczny, indywidualny i masowy. Terroryzm ekonomiczny to akty sabotażu i dywersji, których celem jest spowodowanie szkód i zniszczeń. Metodą działania w tym przypadku są: podpalenia i eksplozje. Terroryzm indywidualny to akty przemocy skierowane przeciwko konkretnym osobom, a metody działania to przede wszystkim porwania, zamachy, mordy polityczne.

[29] Ibidem, s. 23.

[30] Terroryzm w UE. Fakty i liczby, https://www.consilium.europa.eu/pl/infographics/terrorism-eu-facts-figures/, [dostęp: 03.04.2025 r.].

[31] R. Borkowski, *Terroryzm*, [w:] *Konflikty* …, op. cit., s. 132.

[32] Ibidem, s. 117.

Terroryzm masowy polega na skierowaniu aktów przemocy przeciw anonimowym i przypadkowym ofiarom. W tym przypadku terroryści stosują porwania samolotów, przetrzymywanie zakładników, wysadzanie obiektów użyteczności publicznej[33].

Ze względu na przyjętą taktykę walki można wskazać: terroryzm represywny, defensywny i ofensywny. Terroryzm represywny to akty gwałtu i przemocy stosowane przez polityczne reżimy, których celem jest zastraszenie narodu własnego lub okupowanego oraz działania podejmowane przez ruchy polityczne w celu wymuszenia poparcia lub utrzymania jedności. Terroryzm defensywny to akty przemocy stosowane podczas walki z najeźdźcą, ich celem jest obrona istniejących norm i wzorców kulturowych oraz powstrzymanie zmian społecznych. Terroryzm ofensywny oznacza działania, które podejmowane są w celu dokonania różnego rodzaju zmian politycznych oraz społecznych, a metodą działania jest szantaż lub wymuszanie na rządzących podjęcia określonych działań i decyzji, zmieniających istniejący stan[34].

Z uwagi na polityczną strategię można wyróżnić: terroryzm sprawczy bezpośredni, sprawczy pośredni, terroryzm na użytek „propagandy przez czyn". Terroryzm sprawczy bezpośredni to dążenie przez działalność terrorystyczną do obalenia istniejącego porządku i narzucenia własnych idei. Cechuje go przekonanie sprawców o sile i skuteczności podejmowanych działań, a celem ataku są jednostki, na które terroryści chcą wywrzeć wpływ. Terroryzm sprawczy bezpośredni występuje często w trakcie walk ruchów narodowowyzwoleńczych. Celem terroryzmu sprawczego pośredniego jest także dążenie do wprowadzenia zmian politycznych, jednak terroryści nie chcą przejąć odpowiedzialności za rządy w państwie. Jest on zatem formą wymuszenia na władzy ustępstw i zmiany panującego ustroju politycznego, poprzez wprowadzanie dezorganizacji i chaosu. Terroryzm na użytek „propagandy przez czyn" ściśle wiąże się z ruchami rewolucyjnymi. Jego celem jest zgromadzenie jak największej liczby ludzi o podobnych poglądach, burzenie porządku społecznego i informowanie o istnieniu organizacji walczącej o określone idea poprzez zbrodnie i działania destrukcyjne[35].

W oparciu o założenia doktrynalne oraz cele ideologiczne przyjęte przez ruchy terrorystyczne można rozróżnić: terroryzm separatystyczny, nacjonalistyczny, rewolucyjny, islamski, millenarystyczny. Terroryzm separatystyczny

[33] Ibidem, s. 118.

[34] Ibidem, s. 118.

[35] Ibidem, s. 118-119.

obejmuje działania, których celem jest odłączenie od państwa, przeciwko któremu terroryści walczą i utworzenie oddzielnego, własnego lub przyłączenie do innego kraju. Ataki najczęściej kierowane są przeciw wojsku, policji i ich rodzinom, skutkiem tego ma być osłabienie i złamanie woli walki w siłach porządkowych lub wywołanie fali represji i wzrost brutalności funkcjonariuszy wywołany chęcią odwetu. Efektem działań może być wzrost poparcia dla terrorystów ze strony społeczeństwa oraz pozyskanie nowych sił do terrorystycznych ugrupowań. Terroryzm nacjonalistyczny to dążenie do realizacji skrajnie nacjonalistycznych idei prowadzących do wprowadzenia rządów „silnej ręki". Celem terroryzmu rewolucyjnego jest wywołanie rewolucji, która obali istniejący ustrój i powstanie wolnego społeczeństwa. Przyczyną terroryzmu nacjonalistycznego są kryzysy ekonomiczne, polityczne, fiskalne, które powodują wzrost niezadowolenia wśród społeczeństwa, liczne protesty i manifestacje. Destabilizacja ugrupowań rządzących i brak skuteczności wprowadzanych reform w skrajnych przypadkach mogą być powodem aktów przemocy, w tym także aktów terrorystycznych, inicjowanych przez organizacje, których celem jest przejęcie władzy, natomiast przypadkowe ofiary zamachów mają wywoływać dodatkową presję obywateli na ugrupowania rządzące. Terroryzm islamski inspirowany jest przez religijne prawdy Koranu, a jego celem jest walka z niewiernymi oraz utworzenie nowych republik islamskich na wzór Iranu. Świat tak stworzony będzie zaludniony wyłącznie przez ludzi dobrych i czystych pozbawiony wszelkich przejawów zła, ostatecznie stanie się rajem na ziemi. Terroryzm millenarystyczny opiera się na działaniach religijnych sekt, przekonanych, że współczesny świat jest krańcowo zły, a ludzkości grozi kataklizm. Zakłada, że członkowie sekt zostali wybrani, aby utworzyć lepszy świat. Inną formą terroryzmu millenarystycznego jest ekoterroryzm, zakładający, że rozwój cywilizacji i techniki stanowi źródło zła, dozwolone jest każde działanie przeciw cywilizacji[36].

W literaturze przedmiotu funkcjonują inne klasyfikacje pojęcia terroryzm. Ze względu na podmiot prowadzący działalność terrorystyczną Krzysztof Kowalczyk i Wiesław Wróblewski wyróżniają: terroryzm państwowy i terroryzm antypaństwowy. Terroryzm państwowy to zastraszające działania państwa wobec obywateli, różne formy zaangażowania państwa w działalność terrorystyczną, wsparcie finansowe grup terrorystycznych. Terroryzm

[36] Ibidem, s. 119-120.

antypaństwowy to działalność ugrupowań lub pojedynczych osób, których celem jest destabilizacja struktur i porządku publicznego[37].

Przyjmując kryterium motywacji Bożena Zasieczna proponuje podział na: terroryzm polityczny i niepolityczny. Terroryzm polityczny definiowany jest jako działalność terrorystów, którzy kierując się motywami politycznymi, religijnymi bądź ideologicznymi wywołują stan zastraszenia. Wśród rodzajów terroryzmu politycznego wymienia się: terroryzm represywny, subrewolucyjny i rewolucyjny. Terroryzm represywny stosowany jest przez państwo i jego siły porządkowe do stłumienia i podporządkowania określonych grup i jednostek. Terroryzm subrewolucyjny to działalność niewielkich grup lub jednostek motywowanych ideologicznie stosujących przemoc w różnych celach, np. zastraszania, zemsty, które jednak nie są w stanie przeprowadzić fundamentalnych zmian. Celem terroryzmu rewolucyjnego jest rewolucja prowadząca do zasadniczych przemian w strukturze państwa. Terroryzm niepolityczny nie ma powiązania z polityką, władzą, ze względu na motywację działania, można natomiast wyróżnić: terroryzm kryminalny i terroryzm patologiczny. Terroryzm kryminalny to przestępstwa pospolite, popełniane przez sprawców, którzy wykorzystują terrorystyczne metody działania w celu osiągnięcia zysku. Terroryzm patologiczny obejmuje akty terrorystyczne popełniane przez osoby z zakłóceniami czynności psychicznych, których motywacji nie można jednoznacznie ustalić, są one efektem frustracji lub nienawiści odczuwanej wobec określonych osób, grup społecznych lub instytucji[38].

Ze względu na cel ataków terrorystycznych Andrzej Pawłowski wyróżnia: terroryzm indywidualny, ekonomiczny, represyjny, powstańczy, społeczno-rewolucyjny. Terroryzm rewolucyjny to akty przemocy skierowane przeciwko życiu konkretnych osób konkretnie lub osób oznaczonych grupowo. Terroryzm ekonomiczny skierowany jest przeciw zastanym stosunkom gospodarczym, przede wszystkim w prawo wykonywania tytułu własności itp. Terroryzm represyjny stosowany jest przez dominującą grupę społeczną, której przywileje zostają zagrożone. Terroryzm powstańczy to akty terrorystyczne o charakterze etniczno-nacjonalistyczno-separatystycznym. Celem terroryzmu społeczno-rewolucyjnego jest dążenie do zmian systemu politycznego[39]. Ze

[37] K. Kowalczyk, W. Wróblewski, *Oblicza współczesnego terroryzmu*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 60.

[38] B. Zasieczna, (red. nauk.), *Encyklopedia terroryzmu*, Bellona, Warszawa 2004, s. 72.

[39] T. Wałek, *Pojęcie, geneza i* …, op. cit., s. 121.

względu na zasięg terytorialny, terroryzm można podzielić na: międzynarodowy i terroryzm krajowy (wewnętrzny)[40].

Krzysztof Liedel proponuje klasyfikację, wg której terroryzm dzieli się na: terroryzm klasyczny, superterroryzm i cyberterroryzm. Superterroryzm obejmuje terroryzm nuklearny, biologiczny i chemiczny.[41] Cyberterroryzm to „planowany, motywowany politycznie atak przeciw informacji, systemowi komputerowemu, programom i danym komputerowym, który przejawia się w działaniach przeciw celom niewojskowym dokonywanych przez zorganizowane grupy lub tajnych agentów"[42].

Zagrożenie terrorystyczne w Polsce

Na podstawie danych z raportów Global Terrorism Index w 2020 roku Polska znalazła się na 114. miejscu pod względem oddziaływania niebezpieczeństw o charakterze terrorystycznym. W 2019 roku była to pozycja 106., a w 2018 roku – 102. W 2017 roku Polska zajmowała miejsce 109, a z kolei w 2016 było to miejsce najlepsze przez ostatnie 10 lat, czyli 130. Na podstawie danych z przedziału czasowego 2010-2020 największe zagrożenie terrorystyczne dla Polski istniało w 2011 roku, kiedy kraj zajmował 84. miejsce[43].

Postrzeganie przez Polaków zagrożenia terrorystycznego w kraju wiąże się z bieżącą sytuacją na świecie stąd zauważyć można, że poziom lęku podnosi się wraz ze wzrostem liczby ataków terrorystycznych na osoby należące do naszego kręgu kulturowego. Zagrożenie to wzmacnia geopolityczne położenie Polski oraz członkostwo w Unii Europejskiej, w tym przynależność do strefy Schengen. Możliwość swobodnego przekraczania granicy może powodować, że Polska traktowana będzie jako kraj tranzytowy na drodze do zachodniej i północnej Europy, a to z kolei może spotęgować zagrożenia związane z działalnością terrorystyczną. Do czynników zwiększających zagrożenie terrorystyczne zaliczyć można również: udział Polski w misjach pokojowych w Iraku i Afganistanie, sojusz z USA, uczestnictwo w koalicji antyterrorystycznej, przynależność do NATO, kontakty społeczności muzułmańskiej

[40] Ibidem, s. 122.

[41] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2008, s. 35.

[42] R. Cegiełka, *Zagrożenie terroryzmem*…, op. cit., s. 43.

[43] A. Olech, P. Dutkiewicz, *Zagrożenia terrorystyczne dla Francji i Polski*, Wydawnictwo Kontekst, Poznań 2021, s. 86.

w Polsce z przedstawicielami ortodoksyjnych organizacji islamskich bliskich ugrupowaniom ekstremistycznym. Zwraca się również uwagę na obecność dużej liczby osób narodowości czeczeńskiej, często utożsamiającą się pod względem religijnym z ideologią ugrupowań terrorystycznych[44].

Realne wydają się zagrożenia związane z możliwością wykorzystania terytorium Polski do działań o charakterze logistycznym i wspomagającym działalność terrorystyczną. Wśród czynników, które mogą sprzyjać traktowaniu Polski jako zaplecza logistycznego, wymienić można: tranzytowy charakter, infrastrukturę komunikacyjną, kompatybilny z zachodnim system bankowy, liberalną politykę wizową, duże zapotrzebowanie na zagraniczne inwestycje kapitałowe, łatwość zakupu broni i materiałów wybuchowych. Potencjalnym zagrożeniem związanym z działalnością terrorystyczną może być traktowanie przez międzynarodowe organizacje terrorystyczne obszaru Polski jako potencjalnego zaplecza do działań w innych krajach z nią sprzymierzonych bądź sojuszniczych, wykorzystanie polskich instytucji finansowych przez międzynarodowe organizacje do prania pieniędzy, powiązanie przedstawicieli środowisk terrorystycznych ze światem przestępczym w Polsce i łączący się z tym ich udział w działaniach przestępczych, np. w handlu bronią, narkotykami, przemycie ludzi.

Istotną kwestią, w aspekcie potencjalnych zagrożeń dla bezpieczeństwa wewnętrznego, pozostaje problem napływu do Polski uchodźców z regionu Zatoki Perskiej, Afganistanu czy Pakistanu, bowiem są to państwa i regiony o podwyższonym ryzyku terrorystycznym. Odnotowano już przypadki angażowania się tych osób w różnego rodzaju działalność przestępczą, np. przestępstwa związane z towarowym i osobowym ruchem granicznym, legalizowaniem pobytu cudzoziemców w Polsce, wytwarzaniem fałszywych dokumentów, pospolitymi przestępstwami kryminalnymi, przemytem i handlem narkotykami oraz pozyskiwaniem broni, amunicji i materiałów wybuchowych. Zdarzają się również przypadki legalnego wjazdu na terytorium Polski osób, których rzeczywisty cel przyjazdu pozostaje niezgodny z deklarowanym, a Polska jest w tym wypadku wykorzystywana jedynie jako kraj umożliwiający wjazd na obszar Unii Europejskiej[45].

[44] J. Gąsiorowski, *Zagrożenie terrorystyczne Polski – próba oceny zjawiska i sposoby przeciwdziałania atakom w latach 2010-2016*, Kultura Bezpieczeństwa 2019, nr 34, s. 14.

[45] Ibidem, s. 15.

Podsumowanie

Terroryzm w obecnej dobie różni się znacznie od jego wcześniejszych przejawów. Możliwości stworzone przez postęp technologiczny i globalizację, powodują zmianę zasięgu od problemu o skali lokalnej do zagrożenia o charakterze ogólnoświatowym. Wśród badaczy zjawiska funkcjonuje wiele definicji terroryzmu. Niezależnie od przyjętej definicji pojęcia, jest to środek, narzędzie, strategia polityki i jej działanie, zawierający cztery podstawowe elementy: premedytację, motywację lub sprawę, cele, przeważnie niewojskowe oraz konspirację. Celem działalności terrorystycznej jest wpływ na decyzje polityczne, socjalne czy militarne, zmuszenie określonych instytucji lub ludzi do spełnienia postawionych żądań poprzez wytworzenie atmosfery strachu w danej społeczności lub państwie. W ostatnich latach pojawiają się obawy przed tzw. superterroryzmem, który polega na zastosowaniu przez terrorystów broni masowego rażenia lub działań, które mogłyby zdestabilizować sytuację na znacznym obszarze atakowanych państw. Klasyfikację działalności terrorystycznej można przeprowadzić w oparciu o różne kryteria, najczęściej przyjmuje się następujące kategorie: działający podmiot, cel ataku, taktyka walki, polityczna strategia, założenia doktrynalne i cele ideologiczne. Polska nie należy do państw bezpośrednio zagrożonych atakami terrorystycznymi, istnieją jednak przesłanki, że nie można wykluczać zwiększenia zainteresowania Polską ze strony organizacji terrorystycznych.

Literatura

1. Bolechów B., *Terroryzm w świecie podwubiegunowym. Przewartościowania i kontynuacje*, Wydawnictwo Adam Marszałek 2003.
2. Borkowski R., *Terroryzm*, [w:] *Konflikty współczesnego świata*, red. R. Borkowski, Wydawnictwo AG, Kraków 2001, s. 120.
3. Cegiełka R., *Zagrożenie terroryzmem. Poczucie bezpieczeństwa na początku XXI wieku oraz wpływy terroryzmu na procesy gospodarcze w wymiarach mikro i makro*, Agencja Wydawnicza Synergy Elżbieta Meissner, Warszawa 2015.
4. Dunaj B. (red. nauk.), *Słownik Języka Polskiego*, Wydawnictwo Wilga, Warszawa 2005.
5. Gąsiorowski J., *Zagrożenie terrorystyczne Polski – próba oceny zjawiska i sposoby przeciwdziałania atakom w latach 2010-2016*, Kultura Bezpieczeństwa, nr 34, 2019, s. 9-46.
6. *Jak zatrzymać terroryzm: przegląd działań Unii Europejskiej*, https://www.europarl.europa.eu/topics/pl/article/20180316STO99922/jak-zatrzymac-terroryzm-przeglad-dzialan-unii-europejskiej

7. Karolczak K., *Terroryzm XXI wieku – wybrane aspekty*, Terroryzm – studia, analizy, prewencja, nr 1(1), 2022, s. 9-28. https://doi.org/10.4467/27204383TER.22.001.15417
8. Kowalczyk K., Wróblewski W., *Oblicza współczesnego terroryzmu*, Wydawawnictwo Adam Marszałek, Toruń 2006.
9. Kozłowski K. *Terroryzm jako zagrożenie państwa*, [w:] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Dom Wydaw. Elipsa, Warszawa 2009, s. 298-310.
10. Krawczyk A., Wokół definicji terroryzmu, https://histmag.org/Wokol-definicji-terroryzmu-2399.
11. Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawawnictwo Adam Marszałek, Toruń 2008.
12. Madej M., *Międzynarodowy terroryzm polityczny*, Ministerstwo Spraw Wewnętrznych, Warszawa 2001.
13. Olech A., Dutkiewicz P., *Zagrożenia terrorystyczne dla Francji i Polski*, Wydawnictwo Kontekst, Poznań 2021.
14. Szafrański J., *Współdziałanie jednostek obrony terytorialnej i policji w walce z terroryzmem*, Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji, Szczytno 2004.
15. Wałek T., *Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych*, Securitologia, nr 2, 2018, s. 110-124.
16. Zasieczna B. (red.), *Encyklopedia terroryzmu*, Bellona, Warszawa 2004.

dr Łukasz Szymankiewicz
Akademia WSB w Dąbrowie Górniczej
ORCID: 0000-0002-9859-9896
https://doi.org/10.29316/9788368103199_3

PROCES RADYKALIZACJI A TERRORYZM – CASUS BASKIJSKIEJ ORGANIZACJI TERRORYSTYCZNEJ ETA

THE PROCESS OF RADICALIZATION AND TERRORISM – THE CASE OF THE BASQUE TERRORIST ORGANIZATION ETA

Streszczenie

Celem rozdziału jest identyfikacja związku pomiędzy radykalizacją a przechodzeniem od idei narodowo-wyzwoleńczej do brutalnych aktów terroru. Główny problem badawczy sformułowano: w jaki sposób zmieniała się ideologia ETA i jakie miało to przełożenie na taktykę jej działań? Analiza oparta jest na metodzie genealogicznej i porównawczej, co pozwala ukazać trzy kluczowe etapy kształtowania ideologii organizacji: od nacjonalistycznej spuścizny Sabino Arany, przez walkę z reżimem Franco, aż po okres demokratyzacji Hiszpanii i utrwalenie autonomii Kraju Basków. Rozdział ukazuje, jak początkowo pokojowe postulaty i działania koncentrujące się na ochronie kultury baskijskiej, przekształciły się w stosowanie przemocy, początkowo wobec przedstawicieli reżimu, a następnie także wobec celów niemilitarnych, co

Summary

The aim of the chapter is to identify the relationship between radicalization and the transition from the idea of national liberation to brutal acts of terror. The main research problem was formulated: how did ETA's ideology change and how did it translate into the tactics of its activities? The analysis is based on the genealogical and comparative method, which allows us to show the three key stages in the formation of the organization's ideology: from the nationalist legacy of Sabino Arana, through the fight against the Franco regime, to the period of democratization of Spain and the consolidation of the autonomy of the Basque Country. The chapter shows how initially peaceful demands and actions focused on the protection of Basque culture turned into the use of violence, initially against representatives of the regime and then

ostatecznie doprowadziło do utraty poparcia społecznego. Z czasem organizacja zatraciła pierwotny cel i przyjęła taktykę brutalizacji ataków, co paradoksalnie zbliżyło ją do najbardziej radykalnych i brutalnych form terroryzmu globalnego, zrywając z wcześniejszą narodowo-wyzwoleńczą legitymizacją. Głównym wnioskiem z przeprowadzonych analiz jest teza, że proces radykalizacji ETA ukazuje, jak skrajne poglądy i cele niemożliwe do osiągnięcia, mogą prowadzić do eskalacji przemocy i całkowitego odrzucenia norm społecznych, co ostatecznie skutkuje izolacją organizacji i jej upadkiem. Przypadek ETA pozostaje istotnym przykładem dla współczesnych badań nad radykalizacją oraz zagrożeniem terroryzmem.

Słowa kluczowe: terroryzm, radykalizacja, ETA, Kraj Basków i Wolność, nacjonalizm

also against non-military targets, which ultimately led to a loss of public support. Over time, the organization lost its original goal and adopted the tactic of brutalizing attacks, which paradoxically brought it closer to the most radical and brutal forms of global terrorism, breaking with its previous national-liberation legitimacy. The main conclusion of the analysis is that the process of radicalization of ETA shows how extreme views and goals that are impossible to achieve can lead to an escalation of violence and a complete rejection of social norms, which ultimately results in the isolation of the organization and its collapse. The case of ETA remains an important example for contemporary research on radicalisation and the threat of terrorism.

Keywords: terrorism, radicalization, ETA, Basque Country and Freedom, nationalism

Wstęp

Z perspektywy zapobiegania terroryzmowi niebagatelną kwestią jest również zapobieganie radykalizacji[1], ponieważ „nikt nie rodzi się terrorystą. Terrorystą człowiek może się stać poprzez proces radykalizacji”[2]. Dlatego ciekawym studium przypadku jest organizacja, która początkowo stanowczo odrzucała stosowanie przemocy i wywodziła się z patriotycznego kręgu studenckiego wydającego czasopismo promujące baskijską kulturę – szczególnie, jeżeli ostatecznie organizacja ta odpowiada za śmierć kilkuset osób oraz przeprowadzenie ponad dwóch tysięcy ataków terrorystycznych.

Celem niniejszego rozdziału jest zaprezentowanie procesu radykalizacji oraz zmian zachodzących w ideologii baskijskiej organizacji terrorystycznej ETA (bask. *Euskadi Ta Askatasuna*, hiszp. *Pais Vasco i Liberdad*, pol. *Kraj Basków i Wolność*) z perspektywy wyboru celu ataku terrorystycznego. W tym celu niezbędna jest analiza genezy ETA wraz ze zmianami formułowanymi

[1] *EU measures to prevent radicalisation*; https://www.consilium.europa.eu/en/policies/preventing-radicalisation/, [dostęp: 26.04.2025].

[2] *Informacje dot. procesu radykalizacji*; https://tpcoe.gov.pl/cpt/materialy/1799,Informacje-dot-procesu-radykalizacji.html, [dostęp: 26.04.2025].

podczas Zgromadzeń oraz wskazanie metod i celów ataków terrorystycznych. Biorąc pod uwagę metodę genealogiczną można wskazać trzy główne okresy wpływające na ideologię ETA: twórczość Sabino Arany, który był protoplastą baskijskiego nacjonalizmu; funkcjonowanie ETA w okresie reżimu Franco; działalność ETA po 1975 roku. Problem badawczy został sformułowany w formie pytania: jakie zmiany zachodziły w ideologii ETA oraz jaki miały one wpływ na stosowane metody terrorystyczne? Tak dobrany proces badawczy jest niezbędny do wytłumaczenia, dlaczego ETA zmieniła taktykę ataków terrorystycznych i zaczęła wybierać tzw. cele niemilitarne. Umożliwia to również wskazanie okresów, w których ETA cieszyła się poparciem społecznym oraz momentów decydujących o zdyskredytowaniu organizacji wśród hiszpańskiej i baskijskiej opinii społecznej, co przyczyniło się do ostatecznego rozwiązania organizacji.

Analiza zmian zachodzących w ideologii ETA stanowi przykład procesu radykalizacji, który można definiować jako proces, w którym grupa lub osoba przybiera coraz bardziej skrajne poglądy, które mogą prowadzić do ekstremizmu, gdzie ostatnim etapem jest dążenie do stosowania lub chęć stosowania przemocy[3]. Przykładowo, proces radykalizacji opisywany jest za pomocą formy „klatki schodowej o zmniejszającej się liczbie wejść". W tym przypadku radykalizacja przybiera charakter determinizmu, w którym wyróżnia się m.in. następujące fazy: ideologiczne zaangażowanie, radykalizację poglądów, wydarzenie katalizujące, brutalny ekstremizm lub terroryzm[4].

Początki baskijskiego nacjonalizmu

Za protoplastę baskijskiego nacjonalizmu uważa się Sabino Aranę Goiri (1865-1903), który pomimo śmierci w młodym wieku jest autorem wielu prac poświęconych baskijskiej kulturze, szczególnie językowi (*euskera*[5]). W wymiarze politycznym jednym z najważniejszych osiągnięć S. Arany

[3] B. Bolechów, *Radykalizacja do przemocy politycznej. Teorie, mechanizmy, wzorce*, [w:] *Ekstremizm polityczny we współczesnym świecie*, red. A. Moroska-Bonkiewicz, DSWE, Wrocław 2012, s. 55.

[4] D. Muro, *What does Radicalisation Look Like? Four Visualisations of Socialisation into Violent Extremism*, „Notes Internacionals CIDOB", 2016; https://www.cidob.org/en/publications/what-does-radicalisation-look-four-visualisations-socialisation-violent-extremism, [dostęp: 23.04.2025].

[5] W 1888 r. S. Arana opublikował podręcznik do gramatyki pt. *Gramática elemental del euskera bizkaino.*

było założenie 31 lipca 1895 r. Nacjonalistycznej Partii Basków (bask. *Eusko Alderdi Jelzalea*, EAJ; hiszp. *Partido Nacionalista Vasco*, PNV), którą można określić jako chrześcijańsko-demokratyczną partię regionalną[6]. Poglądy polityczne S. Arany i jego stosunek do niepodległości Kraju Basków ewoluowały na przestrzeni lat, na co przynajmniej w początkowej fazie jego życia wpływ miała rodzina. S. Arana wychował się w konserwatywnej i religijnej rodzinie zamożnych baskijskich przedsiębiorców z branży stoczniowej, a jego dziadek i ojciec byli zwolennikami monarchii[7]. Sabino Arana zmienił swoje poglądy w 1882 r. pod wpływem starszego brata Luisa i zainteresował się baskijskim ruchem narodowym[8]. Arana opublikował ponad 300 artykułów, a pierwszym tekstem poruszającym kwestie polityczne był *Pliegos Histórico-Políticos*[9]. Co istotne, w kwestii ewolucji poglądów Arany, praca dotyczyła jedynie jednej prowincji baskijskiej – Vizcai[10]. Pracą, która przyniosła rozgłos Aranie była książka *Bizkaya por su Independencia. Cuatro glorias patrias*. Publikacja ta również dobitnie ukazuje podejście Arany do wybiórczego traktowania historii oraz skłonności do mitologizacji. Joanna Orzechowska-Wacławska wskazuje, że „monografia była właściwie nie tyle pracą historyczną, ile pamfletem historyczno-legendarnym wpisującym się w szeroko rozumiany nurt romantycznej literatury oralnej”[11]. Niemniej jednak prace Arany trafiały na podatny grunt, a sam autor został uznany za głównego nacjonalistę baskijskiego. Dla Arany ważną częścią narodu baskijskiego byli mieszkańcy wsi, ponieważ *euskera* była praktycznie wyłącznie językiem mówionym, nieużywanym w mieście. To mieszkańcy baskijskich wsi i prowincji byli jedynymi nośnikami kultury, przykładowo, najwybitniejsi baskijscy pisarze publikowali swoje dzieła

[6] A. Sroka, *Hiszpańska droga do federalizmu*, Wydawnictwo UWr, Wrocław 2008, s. 269.

[7] J. Orzechowska-Wacławska, *Baskowie. Powstanie współczesnego narodu*, Wydawnictwo UJ, Kraków 2014.

[8] P. J. Chacón Delgado, *El concepto de independencia Vasca en Sabino Arana Goiri*, „Historia Contemporanea”, nr 50, 2014. s. 80-81.

[9] *Una nueva interpretacion de la historia de Bizkaia*; http://www.sabinetxea.org/libro/libro/libro.html, [dostęp: 30.12.2024].

[10] Kraj Basków jako wspólnota autonomiczna składa się z trzech prowincji: Vizcaya, Guipúzcoa, Álava. Historycznie Baskonia składała się z siedmiu prowincji, które obecnie położone są na terenie Hiszpanii i Francji. W skład francuskiej części Baskonii wchodzą trzy prowincje: Lapurdi (franc. Labourd), Zuberoa (franc. Soule), Nafarroa Beherea (franc. Basse-Navarre). Siódmą prowincją jest Navarra, stanowi ona jednak osobną wspólnotę autonomiczną. Stąd wywodzi się jedno z hasło baskijskich nacjonalistów „cztery plus trzy, czyli siedem w jedności”.

[11] J. Orzechowska-Wacławska, *Baskowie. Powstanie współczesnego*…, op. cyt., s. 138.

w języku hiszpańskim[12], co więcej, sam Arana uczył się euskery już jako dorosły[13]. Fundamentami baskijskiego nacjonalizmu S. Arany były: wroga reakcja na industrializację; nacisk na rozwój euskery i kultury baskijskiej; konserwatyzm; katolicyzm; „czystość rasy" i etnocentryzm. Tym samym Arana odrzucał „wszystko co obce" – baskijski nacjonalizm S. Arany przybierał charakter defensywny, a wszelkie działania dążące do dbania o język, „czystość rasy" i propagowanie konserwatywnych poglądów wynikały z obawy przed zmianami, które niosła za sobą industrializacja i modernizacja, szczególnie w kontekście konsekwencji społecznych (np. zagrożenie związane z imigrantami z innych regionów Hiszpanii, gdzie napływ dużej liczby obywateli spoza Kraju Basków mógłby zagrozić przetrwaniu baskijskiego języka, który stanowi nośnik kultury). Istotne jest również, że chociaż historycznie Baskonia składa się z siedmiu prowincji i jest podzielona pomiędzy Hiszpanię i Francję, Arana skupiał się wyłącznie na części hiszpańskiej. Biorąc pod uwagę głoszone przez Aranę poglądy, można wskazać trzy fazy jego ideologicznej ewolucji, które prezentuje tabela 1.

Tabela 1. III fazy ewolucji ideologicznej Sabino Arany

Lata występowania	Cechy charakterystyczne
1893-1898	Radykalne poglądy antyhiszpańskie, antykapitalistyczne i prokatolickie.
1898-1902	Porzucenie antykapitalizmu i ekstremizmu; Arana jako przemysłowiec; poglądy prokatolickie.
1902-1903	Postawa prohiszpańska, Kraj Basków jako autonomia; poglądy prokatolickie.

Źródło: opracowanie własne.

Jedyną niezmienną cechą charakteryzującą poglądy S. Arany był pozytywny stosunek do religii. Pierwszy etap jego zaangażowania w sprawę baskijskiej niepodległości charakteryzował się najbardziej radyklaną postawą i wrogością do Hiszpanii. W drugim okresie odejście od ekstremizmu i antykapitalizmu podyktowane jest osobistymi zmianami w życiu Arany, który sam stał się przemysłowcem. Pod koniec życia S. Arana głosił poglądy prohiszpańskie, samemu określając je jako *evolución españolista*, wskazując jednocześnie na konieczność odrzucenia dążeń niepodległościowych i obranie za cel

[12] T. Mikołowski, P. Machcewicz, *Historia Hiszpanii*, Zakład Narodowy im. Ossolińskich, Wrocław 2009, s. 314.

[13] E. Hobsbawm, *Narody i nacjonalizm po 1870 roku. Program, mit i rzeczywistość*, Wydawnictwo Difin, Warszawa 2010, s. 128.

utworzenie autonomii w ramach państwa hiszpańskiego[14]. Hiszpański historyk Santiago de Pablo wskazuje, że niektórzy baskijscy nacjonaliści próbowali bagatelizować tę „hiszpańską ewolucję Arany", przedstawiając ją jedynie jako zmianę taktyki, a nie jako rezygnację z ostatecznego celu, jakim w dalszym ciągu byłaby niepodległość. Ewolucja ta, przedstawiona w bardzo sprzeczny sposób, nigdy nie została zakończona, ponieważ w wyniku śmierci Arana pozostawił nieokreślony zakres swojej ostatniej myśli – nagła zmiana poglądów i niewystarczające wytłumaczenie były powodem kontrowersji wśród jego własnych zwolenników[15], jednak co istotne dla politycznego kształtu Kraju Basków, PNV w przeciwieństwie do ETA przejęła od Arany pogląd o dążeniu wyłącznie do autonomii.

Geneza ETA

Za oficjalną datę utworzenia ETA uznaje się 31 lipca 1959 roku, jednak proces powstawania baskijskiej organizacji terrorystycznej trwał co najmniej kilka lat. W 1953 r. z inicjatywy studentów z Bilbao powstało czasopismo *Ekin* (pol. Działać), które następnie przekształciło się w tajne stowarzyszenie. *Ekin* przejął idee niepodległościowe S. Arany z jego pierwszej, radykalnej fazy, tzw. *sabiniano*. Anna Antczak wskazuje, że oprócz *Ekin*, zalążkiem ETA były również dwa radyklane ugrupowania charakteryzujące się bezkompromisowymi poglądami na temat niepodległości Baskonii – *Jagi-Jagi* oraz *Aberri*[16]. Nazwa czasopisma i radykalne poglądy *Aberri* i *Jagi-Jagi,* nie są przypadkowe. Z powodu dyktatury, liderzy PNV przebywali na emigracji i charakteryzowała ich bierność oraz bezradność – to właśnie bierna postawa PNV była czynnikiem katalizującym i konsolidującym przyszłych członków ETA. Symboliczna jest oficjalna data powstania ETA – 31 lipca, to również dzień powstania PNV. ETA również przejęła znaczną część radykalnych poglądów Arany z jego pierwszej fazy działalności politycznej; utworzenie ETA 31 lipca

[14] A. Antczak, *Separatyzm baskijski*, Sprawy Narodowościowe, nr 37, Warszawa 2010, s. 151.

[15] S. De Pablo, *El nacionalismo vasco ante el Estado español (1895-1937)*, Studia historica. Historia contemporánea, nr 18, 2000, s. 79-93.

[16] A. Antczak, *Kształtowanie się tożsamości narodowej wspólnot autonomicznych w Hiszpanii*, AON, Warszawa 2008, s. 99.

to symboliczne przesłane do PNV – „młodzi nacjonaliści baskijscy nie potrzebują wsparcia partii, aby kontynuować tradycje nacjonalizmu *sabiniano*[17].

Daniele Conversi wskazuje, że ETA nie od razu powstała jako typowa organizacja terrorystyczna, ale raczej jako ruch studencki, a baskijski nacjonalizm był radykalny, ale nie stosował przemocy[18]. Studenci chcieli poznawać historię swojej społeczności lokalnej, dyskutować, organizowali spotkania, na których wywieszali baskijską flagę oraz inne symbole narodowe, tym samym organizacja początkowo skupiała się na dbaniu o baskijską kulturę, w tym język – w tych aspektach widać zbieżność z ideologią Arany[19].

Z czasem ETA deklarowała chęć utworzenia Baskonii jako niepodległej republiki socjalistycznej[20], odrzucała idee rasowe Arany oraz głosiła poglądy antyklerykalne, mianowicie rasizm zastąpiono etosem wyrażającym się dbaniem o kulturę i język, religię zastąpiono nacjonalizmem i redefiniowano cały ruch jako patriotyczny i bezwyznaniowy[21]. Porównując poglądy S. Arany i ETA należy wskazać, że Arana był przeciwnikiem socjalizmu twierdząc, że nacjonalizm baskijski i socjalizm są niemożliwe do pogodzenia[22]. Z jednej strony powstanie ETA konsolidowało tych baskijskich nacjonalistów, których charakteryzowała chęć działania na rzecz niepodległości i walki z reżimem; z drugiej strony z perspektywy władzy centralnej powstanie ETA osłabiało najsilniejsze baskijskie ugrupowanie, jakim była konserwatywna PNV[23]. W początkowej fazie swojej działalności ETA sama definiowała się jako organizacja rewolucyjna i socjalistyczna, której celem jest dążenie do narodowego wyzwolenia całej Baskonii. Z perspektywy analizy nurtów terrorystycznych, jak najbardziej można uznać ETA za organizację terrorystyczną o charakterze

[17] A. Llanos-Antczak, *Separatyzm baskijski. Historia, współczesność, perspektywy*, Dom Wydawniczy Elipsa, Warszawa 2019, s. 49.

[18] D. Conversi, *Sovereignty, boundaries and violence. Constructing the Basque national self (1959-2011)*, [w:] *Sovereignty Revisited. The Basque case*, red. nauk. I. Güell, P. Åshild, Kolås Åshild, Routledge, Londyn 2017, s. 20-21.

[19] S. Jeram, D. Conversi, *Deliberation and Democracy at the End of Armed Conflict. Post-Conflict Opportunities in the Basque Country*, [w:] Democratic Deliberation in Deeply Divided Societies. From Conflict to Common Ground, red. nauk. J. Ugarizza, D. Clauwaerts, Palgrave Macmillan, Basingstoke 2014, s. 55.

[20] D. Conversi, *Sovereignty, boundaries and*…, op. cit., s. 21.

[21] F. Letamendia Belzunde, *Historia de Euskadi. El nacionalismo vasco y ETA*, Ruedo Iberico, Paryż 1975, s. 279.

[22] J. J. Solozábal Echavarria, *El primer nacionalismo vasco. Industrialismo y conciencia nacional*, Tucar Ediciones, Madryt 1975, s. 339.

[23] S. Jeram, D. Conversi, *Deliberation and Democracy*…, op. cit.

wyzwoleńczym[24], chociaż należy mieć na uwadze, że początkowo ETA taką organizacją nie była, a jej członkowie stanowczo odrzucali stosowanie przemocy.

Ideologia ETA w okresie dyktatury

Lata 1962-1970 były kluczowe w aspekcie krystalizowania się ideologicznej bazy ETA. W tym okresie wyróżnia się sześć Zgromadzeń ETA, które charakteryzowały się odmienną ideologią oraz pomysłami dotyczącymi stosowania strategii i taktyki działań terrorystycznych. Na zewnątrz ETA cieszyła się opinią organizacji homogenicznej, jednak cały proces wewnętrznej transformacji był burzliwy, wśród członków występowały różne opinie na temat głównych metod i celów walki, a także odmienne poglądy polityczne. W tym okresie na zmiany zachodzące wewnątrz ETA wpływ miały dwa główne czynniki. Po pierwsze, zmiany społeczne w Hiszpanii i Kraju Basków wynikające z industrializacji i modernizacji, które sprawiały, że do Kraju Basków, jako bogatszego regionu, zaczęła przybywać coraz większa liczba migrantów, zwłaszcza robotników. Po drugie, wśród członków ETA widoczna była fascynacja ruchami rewolucyjnymi i antykolonialnymi[25], szczególnie w aspekcie stosowanych metod prowadzenia walki.

Jak wspomniano we wcześniejszej części niniejszej pracy, ETA dość szybko zdefiniowała się jako organizacja patriotyczna i bezwyznaniowa (oficjalnie już trzy lata po powstaniu, w 1962 r.), chociaż stanowiło to formę kompromisu pomiędzy dwiema głównymi frakcjami: patriotów głoszących konieczność walki o sprawę narodową oraz „rewolucjonistów". Z perspektywy zagrożeń terrorystycznych kluczowe było drugie Zgromadzenie ETA w 1963 r., gdy ogłoszono, że ETA „wchodzi na ścieżkę przemocy". Przeforsowano również idee tzw. „wojny rewolucyjnej", na wzór wydarzeń na Kubie oraz w Algierii; w tym roku również zwrócono uwagę na coraz większe znaczenie klasy robotniczej[26]. ETA zaczerpnęła z myśli baskijskiego filozofa Federico

[24] V. Grotowicz, *Terroryzm w Europie Zachodniej*, Wydawnictwo Naukowe PWN, Warszawa 2000.

[25] D. Conversi, *The Left and nationalism. From the French Revolution to the Anthropocene*, [w:] *Research Handbook on Nationalism*, red. L. Greenfeld, Z. Wu, Edward Elgar, Northampton 2020, s. 38.

[26] D. Conversi, G. Espiau, *Basque*, [w:] *Comparing Peace Processes*, A. Ozerdem, R. Mac Ginty, Routledge, Londyn-Nowy Jork 2019, s. 57

Krutwiga, który w swojej książce *Vasconia* wydanej w 1963 r. w Argentynie stwierdzał, że nie należy bać się industrializacji, ponieważ ona zapewnia niezbędny rozwój i dynamizm, również w aspekcie kultury[27]. Natomiast napływ klasy robotniczej bez wątpienia stanowił zagrożenie dla baskijskiej kultury, dlatego właśnie tak istotne było odejście od sabinowskiej czystości rasy na rzecz baskijskiego etosu, gdzie za Baska można uznać osobę znającą euskere. Ponadto klasa robotnicza stanowiła potencjalną dużą grupę nowych zwolenników ETA.

Podczas trzeciego Zgromadzenia poruszano m.in. kwestię emancypacji klasy robotniczej, co można uznać za kontynuację wcześniejszych postanowień. Zauważalne było forsowanie coraz bardziej bezkompromisowych poglądów, co przejawiało się w szerzeniu idei antykapitalistycznych i antyimperialnych. W kwestii organizacyjnej, doszło do podziału na cztery sekcje: militarną, aktywistów, informacyjną oraz biuro polityczne. Podczas czwartego Zgromadzenia wprowadzono taktykę walki „akcja-represje-akcja", charakteryzującą się prowokacyjną działalnością ETA, która tym samym chciała wpływać na zakorzenienie w świadomości nie tylko Basków, ale wszystkich Hiszpanów i opinii międzynarodowej, że Baskowie są narodem uciskanym, a władza centralna jest oprawcą. Tym samym każdy kolejny atak terrorystyczny prowadziłby do represji i akcji odwetowych ze strony frankistowskiego reżimu, w związku z czym w opinii ETA następna akcja byłaby nie formą odwetu, a obrony przed uciskiem. W trakcie czwartego Zgromadzenia po raz kolejny podkreślono konieczność walki o przetrwanie euskery i baskijskiej kultury. Co istotne, wielu członków ETA działało w sferze kultury, prowadząc m.in. lekcje języka baskijskiego[28]. Podczas piątego Zgromadzenia z 1965 r. doszło do konsolidacji idei walki niepodległościowej z walką o klasę robotniczą, czego wyrazem stała się koncepcja „*Pueblo Trabajador Vasco*" (pol. baskijski lud pracy). W tym okresie ETA podjęła współpracę ze związkami zawodowymi, w tym z prokomunistycznym, nielegalnym i działającym tajnie związkiem zawodowym *Comisiones Obreros*[29]. Współpraca ta wymusiła wprowadzenie dyscypliny i tajności spotkań, przez co *etarras*[30] musieli podejmować jednoznaczne decyzje, co do dalszego członkostwa w organizacji. Natomiast kon-

[27] F. Krutwig, *Vasconia*, Norbait, Buenos Aires 1973.

[28] K. Mirgos, *Obcy i nowi Baskowie. Migracje, tożsamość i języki w Baskijskiej Wspólnocie Autonomicznej*, Wydawnictwo UG, Gdańsk 2018, s. 190-191.

[29] J.M. Garmendia, *Historia de ETA*, Haranburu, San Sebastian 1979.

[30] *Etarras* – tym określeniem nazywano członków ETA.

sekwencją konspiracyjnego działania ETA było powstawanie nowych grup o własnych poglądach, co sprzyjało powstawaniu konfliktów ideologicznych.

Następne lata to okres konfliktów wewnętrznych, gdzie dochodziło do podziałów na różne frakcje. Duże napięcie wywoływały nie tylko wewnętrzne spory ideologiczne, ale również represje ze strony władzy, które były odpowiedzią na ataki terrorystyczne. W wyniku aresztowań w latach 1968-1970, ETA była zmuszona do wymiany niemal całego kierownictwa, co również negatywnie wpływało na sytuację wewnętrzną baskijskiej organizacji. Naprzeciw siebie stawały frakcje głoszące konieczność nadania priorytetu walce o klasę robotniczą; frakcje chcące pogodzić walkę robotniczą z walką narodowowyzwoleńczą; grupy głoszące, że jedyną opcją stawiania oporu władzy jest stosowanie przemocy. W 1970 r. doszło do VI Zgromadzenia, które było najbardziej kontrowersyjne i doprowadziło do rozłamu. W 1971 r. skonfliktowane frakcje doszły do porozumienia i uznano, że zamachy terrorystyczne i walka zbrojna to jedyne metody walki[31]. A. Llanos-Antczak uważa, że spory wewnętrzne w późniejszych latach nie miały charakteru ideologicznego i dotyczyły wyłącznie aspektu strategicznego i taktycznego, np. rozłam w 1974 r. na ETA militarną – ETA-m – i ETA polityczno-militarną – ETA-pm[32], niemniej jednak z perspektywy zagrożeń terrorystycznych zmiany te były również istotne.

Tabela 2. Zgromadzenia ETA w latach 1962-1965

Nr zgromadzenia	Rok	Główne założenia ideologiczne
I	1962	ETA jako organizacja patriotyczna i bezwyznaniowa.
II	1963	Odwołanie do ruchów rewolucyjnych i antykolonialnych w Trzecim Świecie, np. na Kubie i w Algierii, tzw. „wojna rewolucyjna". Ogłoszenie wejścia na „ścieżkę przemocy". Zwrot w kierunku klasy robotniczej i industrializacji.
III	1964	Antyimperializm, antykapitalizm, emancypacja klasy robotniczej. Podział ETA na cztery sekcje: militarną, aktywistów, informacyjną, biuro polityczne.
IV	1965	Walka klas i walka o niepodległość. Teoria walki „akcja-represje-akcja". Konieczność przetrwania języka i kultury.
V	1965	Kombinacja nacjonalizmu i walki klasy robotniczej – współpraca ze związkami zawodowymi; stosowanie konspiracji.
VI	1970	Największy konflikt wewnętrzny. Rozłam. Ideologiczne porozumienie w 1971 r. – ustalenie, że zamachy terrorystyczne i walka zbrojna to jedyne metody walki.

Źródło: opracowanie własne.

[31] A. Llanos-Antczak, *Separatyzm baskijski. Historia*…, op. cit., s. 60-61.

[32] Ibidem, s. 62.

Zmiany zachodzące w ETA w latach 1962-1971 można określić jako dopracowywanie własnej ideologii, szukanie optymalnej strategii politycznej oraz taktyki prowadzenia walki. Każda następna zmiana była konsekwencją wcześniej obranych kierunków. Można powiedzieć, że był to konsekwentny proces radykalizacji, zmierzający ostatecznie w stronę stosowania metod terrorystycznych i ogólnie terroryzmu, jako narzędzia politycznego. Do końca frankistowskiego reżimu ETA nie przechodziła już zmian ideologicznych. Katalizatorami zmian były dopiero śmierć gen. Franco w 1975 r., której konsekwencją był upadek reżimu; proces demokratyzacji Hiszpanii, gdzie kluczowe było ustanowienie w 1978 r. konstytucji, w której zapisano prawo do tworzenia autonomii oraz właśnie powstanie w 1979 r. autonomii Kraju Basków. W tym okresie odnotowano jedną istotną zmianę w kontekście ETA, która miała miejsce w 1981 roku, gdy część *etarras* uznała, że nastąpił czas na zakończenie walki zbrojnej/terrorystycznej, ponieważ demokracja umożliwia stosowanie innych, legalnych metod politycznych. Tym samym ETA-pm ogłosiła zawieszenie walk, a część jej członków rozpoczęła legalną działalność polityczną. Natomiast ETA-m kontynuowała walkę, ukazując również fanatyzm tej frakcji.

Ideologia ETA a cele i metody ataków terrorystycznych oraz konsekwencje ataków

Zgodnie z ostatnim raportem z 2018 r. opublikowanym przez kierownictwo ETA, organizacja ta przeprowadziła 2606 ataków i zabiła 758 osób, z czego 727 ataków wymierzonych było w policję, Guardia Civil oraz wojsko (łącznie 437 ofiary śmiertelne)[33]. Jednak na przestrzeni lat dochodziło do zmian stosowanych metod i wyboru celu ataku.

Posiłkując się danymi z Global Terrorism Database, w latach 1970-1975 przeprowadzono 55 ataków, w których zginęły 34 osoby; w latach 1976-1979, a więc w początkowej fazie kształtowania się hiszpańskiej demokracji oraz autonomii Kraju Basków ETA przeprowadziła 361 ataków, w których zginęło

[33] Oficjalne dane MSW Hiszpanii podają 863 ofiary, natomiast Hiszpańska Wspólnota Ofiar Terroryzmu Covite informuje o 829 ofiarach. Zob.: Hiszpania: ETA ujawniła łączny bilans swoich zamachów, Gazeta Prawna, [dostęp: 06.11.2018], https://www.gazetaprawna.pl/wiadomosci/artykuly/1336508,eta-o-liczbie-zamachow.html, [dostęp: 01.01.2024].

146 osób, natomiast po 1981 r. odnotowano ponad 1300 ataków[34]. Jak wspomniano wcześniej, ETA początkowo odrzucała przemoc, pierwsze akty przemocy miały miejsce w 1961 r. i stanowiły formę sabotaży. W 1965 r. ETA przeprowadziła pierwszy napad na bankowóz, natomiast pierwszego zabójstwa politycznego dokonano w 1968 r. – ofiarą był oficer hiszpańskiej policji Melitón Manzanas. W tym samym roku, w wyniku wymiany ognia podczas kontroli drogowej, zginął pierwszy *etarras*, co wywołało nielegalne demonstracje poparcia dla ETA[35], również zabójstwo Manzanasa, który znany był z okrucieństwa i stosowania tortur, zostało pozytywnie odebrane przez część hiszpańskiej społeczności. W 1968 r. władze centralne zaostrzyły represje wobec ETA, w 1969 r. w prowincjach baskijskich aresztowano ok. 2 tysiące osób; w 1970 r. na trzy miesiące wprowadzono stan wyjątkowy[36]. Natomiast w Burgos odbył się pokazowy proces najważniejszych członków ETA, w wyniku którego dziewięciu *etarras* otrzymało wyroki śmierci, jednak cały proces zamiast zastraszyć ETA, stał się dla niej katalizatorem do dalszych działań, ponieważ międzynarodowa opinia publiczna zdecydowanie potępiła stosowane przez Franco represje, w wyniku czego wyroki śmierci zamieniono na 30 lat pozbawienia wolności. Wewnątrz Hiszpanii w obronie ETA wystąpili nie tylko Baskowie, ale również część hiszpańskiego społeczeństwa, kler oraz nawet część wojska[37].

Od 1968 r. celem ataków terrorystycznych ETA stali się przedstawiciele władzy, przede wszystkim policjanci, żołnierze i politycy. Biorąc pod uwagę koncepcję czterech fal współczesnego terroryzmu Davida Rapaporta[38], ideologię ETA oraz cele ataków, organizacja wpisywała się w drugą (antykolonialną) i trzecią (lewicowo-separatystyczną) falę współczesnego terroryzmu. Tym samym, z perspektywy nurtów terroryzmu, działania ETA były logiczne, co więcej można było wskazać pewnego rodzaju samoograniczenia,

[34] Różne źródła podają odmienne dane dotyczące liczby ataków oraz ofiar, dlatego autor w niniejszej pracy podał oficjalne, ale zapewne zmanipulowane dane pochodzące od ETA oraz dane pochodzące z wiarygodnego źródła, jakim jest Global Terrorism Database.

[35] D. Conversi, G. Espiau, *Basque*…, op. cit., s. 58; P.R. Clark, *The Basque insurgent. ETA, 1952-1980*, University of Wisconsin Press, Madison 1984, s. 49.

[36] T. Miłkowski, P. Machcewicz, *Historia Hiszpanii*, Zakład Narodowy Im. Ossolińskich, Wrocław 2009, s. 381.

[37] A. Llanos-Antczak, *Separatyzm baskijski. Historia*…, op. cit., s. 61.

[38] D. C. Rapaport, *The Four Waves of Modern Terrorism*, [w:] *Attacking Terrorism Elements of a Grand Strategy*, A. K. Cronin, J. M. Ludes (red. nauk.), Georgetown University Press, Waszyngton 2004.

tj. selektywność doboru celu i metod ataku, ograniczały ryzyko zabicia osób postronnych.

W 1972 r. ETA zaczęła wybierać również tzw. cele niemilitarne, gdzie jedną z ofiar był przedsiębiorca Lorenzo Zabala[39] – obieranie za cel przedstawicieli bogatych przedsiębiorców wynikało z chęci zwiększenia poparcia wśród klasy robotniczej. Szczyt swojej popularności ETA osiągnęła w 1973 r., po udanym ataku na premiera Hiszpanii, admirała Luisa Carrero Blanco. W tym przypadku część hiszpańskiego społeczeństwa, która nie popierała reżimu uważała, że ETA wystąpiła również w ich imieniu. Biorąc pod uwagę zabójstwo premiera, niewielka liczba ataków terrorystycznych w okresie dyktatury podyktowana była raczej selektywnym doborem celów ataku i chęcią ograniczenia ofiar postronnych niż skutecznością frankistowskiego reżimu. Był to nadal okres, w którym ETA wypracowywała swoją ideologię; znamienne jest, że między V a VI Zgromadzeniem w ETA dochodziło do największych konfliktów wewnętrznych, szczególnie dotyczących właśnie stosowania przemocy. W tym przypadku istotne były demonstracje poparcia oraz pokazowy proces w Burgos. Wyraźne poparcie jakie ETA otrzymała nie tylko ze strony Basków i Hiszpanów, ale również ze strony społeczności międzynarodowej mogło zostać zinterpretowane przez ETA jako przyzwolenie na stosowanie przemocy w „szczytnym celu". Z pewnością obierając od samego początku za cel tzw. cele miękkie oraz zabijając osoby postronne, ETA takiego poparcia by nie otrzymała, czego najlepszym przykładem są późniejsze ataki i ich konsekwencje.

Od około 1977 r. ETA zaczęła stosować taktykę *muertes sin precedences*, gdzie głównymi celami ataków byli politycy z różnych partii politycznych, aktywiści i przedstawiciele świata nauki. Była to nadal wąska grupa osób, jednak coraz częściej nie byli to przedstawiciele władz. Nasilona liczba ataków w latach 1976-1979 była argumentowana chęcią zatrzymania niekorzystnego w opinii ETA procesu konstytucyjnego[40] oraz tworzenia autonomii Kraju Basków. Po pierwsze, ETA chciała całkowitej niepodległości, co było celem niemożliwym do osiągnięcia. Po drugie, ustanowienie autonomii Kraju Basków sprawiłoby, że ETA straciłaby rację bytu. Oba wskazane powody argumentują również stawianie przez ETA nierealnych żądań podczas

[39] R. Darby, *Legitimate Targets. A Control or Violence?*, [w:] *New Perspectives on the Nothern Ireland Conflict*, red. A. Guelke, Avebury, Aldershot 1994, s. 46-64.

[40] E. Górski, *O demokracji w Hiszpanii (1975-1995)*, Wydawnictwo Instytutu Filozofii i Socjologii PAN, Warszawa 1997, s. 21.

negocjacji z rządem Hiszpanii. Można stwierdzić, że w pewnym momencie *etarras* chcieli prowadzić walkę dla samej walki, a nie realizacji pierwotnych celów, do jakich ETA została powołana.

Jednym z przełomowych ataków, który nie tylko spowodował spadek poparcia dla ETA, ale wręcz zaktywizował obywateli Hiszpanii do wyrażenia swojego sprzeciwu, był atak bombowy na centrum handlowe Hipercor w Barcelonie z 19 czerwca 1987 roku. ETA podłożyła na parkingu pod centrum handlowym improwizowany ładunek wybuchowy w samochodzie-pułapce, tzw. VBIED – ang. *vehicle-borne improvised explosive device*[41]. W wyniku ataku zginęło 21 cywili, a ETA zaczęła tracić poparcie społeczne[42]. Był to jeden z momentów obrania za cel osób postronnych na zasadzie braku selekcji, chociaż dopiero w 1995 r. ETA ogłosiła stosowanie nowej taktyki „społecznego cierpienia". Próby kolejnych ataków spotykały się z coraz większym niezadowoleniem społecznym i falami protestów, również wśród Basków. Wydarzeniem, w wyniku którego ETA straciła ostatecznie poparcie nie tylko w Hiszpanii i Kraju Basków, ale również wśród społeczności międzynarodowej, było porwanie i zabójstwo w 1997 r. polityka prawicowej partii Partido Popular, Miguela Ángel Blanco Garrido. ETA za cel ataków obierała również hiszpańską branżę turystyczną, co także było odbierane negatywnie.

Analizując ataki ETA począwszy od lat 80' XX w., do ostatniego ataku z 2011 r,. zauważyć można brak zgodności z cechami charakterystycznymi dla organizacji narodowowyzwoleńczej. W okresie dyktatury frankistowskiej ETA stosowała improwizowane urządzenia wybuchowe (IED, ang. *improvised explosive device*), np. podczas zabójstwa admirała Blanco, dokonywała uprowadzeń i zabójstw politycznych z użyciem broni palnej, ale nie dokonywała ataków na osoby postronne, a jej ataki nie przybierały tak brutalnej formy, jak w późniejszym okresie aktywności. Atakowanie tzw. celów miękkich, np. dużych skupisk ludzi w centrach handlowych przy użyciu IED, brak selekcji celów ataków, dążenie do spowodowania jak największych strat materialnych, stanowią cechy charakterystyczne terroryzmu motywowanego ideologią religijną. Zdaniem autora, tak drastyczna zmiana celów ataku wynika nie tylko z radykalizacji politycznej, ale również z konieczności poszukiwania nowych bodźców w celu zwrócenia uwagi na sprawę, o którą walczą

[41] Ł. Szymankiewicz, *The modus operandi of terrorist attacks using improvised explosive devices in landside zones from 2001-2018*, Journal of KONBiN, vol. 52, iss. 3, 2022 s. 133.

[42] M. Kuczyński, *Krwawiąca Europa. Konflikty zbrojne i punkty zapalne w latach 1990-2000. Tło historyczne i stan obecny*, Bellona, Warszawa 2001, s. 357.

terroryści, ponadto poszerzanie celów ataku np. o przedsiębiorców, miało na celu zdobycie nowych zwolenników, np. z klasy robotniczej. Należy pamiętać, że terroryzm stanowi metodę przekazywania społeczeństwu i władzy komunikatów – dlatego, im atak terrorystyczny będzie bardziej spektakularny, tym większe grono obiorców usłyszy komunikat. Być może ETA obawiała się, że w dobie terroryzmu samobójczego i ataków, w których giną setki cywili, ich komunikaty wysyłane w formie ataków polegających na podkładaniu ładunków wybuchowych, a następnie powiadamianiu służb o planowanym ataku – czyli przeprowadzeniu ataku, w którym z założenia nikt nie powinien zginąć – nie będą w ogóle docierać do odbiorców. To jest wyłącznie przypuszczenie wynikające z analizy historii ETA, jej zmian ideologicznych i przeprowadzonych ataków. Idąc tym tokiem myślenia i opierając się wyłącznie na doborze celów ataków, *etarras* posiadali dwa wyjścia: zaniechać przeprowadzania ataków, a tym samym rozwiązać ETA lub zwiększyć brutalizację ataków. Wybór drugiej opcji był równoważny z uznaniem przez ogół społeczeństwa hiszpańskiego ETA za takie samo zagrożenie, jak organizacje typu Al-Kaida. Dobitnym przykładem na potwierdzenie powyższej tezy jest największy w historii atak terrorystyczny przeprowadzony na terenie Unii Europejskiej, który miał miejsce 11 marca 2004 r. w Madrycie, a w wyniku, którego śmierć poniosło 191 osób. Początkowo za atak obarczono ETA, chociaż specjaliści szybko wskazywali, że metody ataku nie pasują do taktyki Basków, a w późniejszym czasie do ataku przyznała się Al-Kaida[43]. Mimo to, fale sprzeciwu i protestów nawołujących do rozwiązania ETA, przelały się niemal przez całą Hiszpanię, w tym również przez Kraj Basków. Paradoksalnie atak, za który nie odpowiadała ETA przyczynił się do utraty resztek poparcia społecznego dla tej organizacji terrorystycznej. Być może, gdyby ETA ograniczyła się wyłącznie do selektywnych ataków na przedstawicieli władzy, a połowy jej ofiar nie stanowiliby cywile, poparcie społeczne dla organizacji byłoby wyższe, nawet po utworzeniu autonomii.

Podsumowanie

ETA stanowi bardzo dobry przykład radykalizacji grupowej, gdzie widoczny jest szczególnie niebezpieczny proces podejmowania coraz bardziej

[43] I. Szkurłat, *Terroryzm a polityka bezpieczeństwa państw Europy Zachodniej na przełomie XX i XXI wieku*, Wydawnictwo Naukowe Akademii Pomorskiej w Słupsku, Słupsk 2018, s. 135-136.

skrajnych działań, w celu walki o niemożliwy do zrealizowania cel. W przypadku ETA jest to szczególnie widoczne w atakach przeprowadzanych już po utworzeniu autonomii Kraju Basków, gdzie coraz brutalniejszy dobór celów i metod terrorystycznych uniemożliwiał ETA cofanie się w swoich nierealnych żądaniach i w praktyce stanowił drogę donikąd. Przypadek ten wskazuje również na zagrożenie radykalizacją osób lub grup, które początkowo nie biorą pod uwagę stosowania przemocy. W przypadku ETA wypracowanie własnej ideologii było procesem żmudnym i długotrwałym. Ostatecznie powstała organizacja antyklerykalna, antyimperialna, dążąca do ustanowienia niepodległej republiki Basków o ustroju socjalistycznym. Również w przypadku wyboru metod walki o niepodległość widoczny był kilkuletni proces ewolucji, gdzie początkowe odrzucenie przemocy przechodziło w stronę stosowania sabotażu, organizowania napadów na bankowozy, uprowadzeń, zabójstw politycznych, aż po obieranie tzw. celów miękkich. Analizując historię ETA, zauważalne są dwa okresy charakteryzujące się diametralnie różnym poparciem społecznym. W czasie dyktatury Franco ETA była symbolem walki z reżimem, nie tylko w opinii samych Basków, ale również części społeczeństwa hiszpańskiego, sprzeciwiającego się dyktaturze. Być może, gdyby w 1981 r. wszyscy *etarras* postąpili tak samo jak członkowie ETA-pm, ETA cieszyłaby się statusem legendarnej organizacji, która wymierzała sprawiedliwość nadużywającym władzy funkcjonariuszom (np. zabójstwo Manzanasa w 1968 r.), a zabijając w 1973 r. premiera Blanco zmieniła bieg historii i przyczyniła się nie tylko do utworzenia autonomii Kraju Basków, ale również do demokratyzacji Hiszpanii. Tymczasem fanatyczna postawa ETA-m oraz obieranie za cel cywili, przedstawicieli sceny politycznej z obozów niesprawujących władzy, aktywistów czy każdej innej osoby, która nie popierała ETA, doprowadziły do osamotnienia i powolnego upadku organizacji, gdzie przedłużająca agonia spowodowała śmierć wielu niewinnych osób, a nierealny cel nigdy nie mógł zostać osiągnięty. Dopiero w 2018 r. ETA ogłosiła ostateczne rozwiązanie wszystkich struktur, a w krótkim komunikacie lakonicznie przeprosiła za krzywdy wyrządzone cywilom, stwierdzając jednocześnie, że zabójstwa funkcjonariuszy, żołnierzy i polityków były jak najbardziej usprawiedliwione. W ostatnim komunikacie dowództwo ETA napisało: „*ETA surgió de este pueblo y ahora se disuelve en él*”[44] co można przetłumaczyć jako „ETA wyrosła z ludu i teraz

[44] Treść informacji ETA o samorozwiązaniu zob.: A. Terradillos, *ETA anuncia su disolución*, „Ser” 03.05.2018; https://cadenaser.com/ser/2018/05/03/politica/1525346984_523675.html, [dostęp: 01.01.2024].

wraca do ludu". Pytanie tylko, czy po tylu latach bezsensownej przemocy i cierpienia, lud przyjąłby *etarras*.

Literatura

1. Antczak A., *Kształtowanie się tożsamości narodowej wspólnot autonomicznych w Hiszpanii*, AON, Warszawa 2008.
2. Antczak A., *Separatyzm baskijski*, Sprawy Narodowościowe, nr 37, 2010, s. 149-161.
3. Bolechów B., *Radykalizacja do przemocy politycznej. Teorie, mechanizmy, wzorce*, [w:] *Ekstremizm polityczny we współczesnym świecie*, red. A. Moroska-Bonkiewicz, Wydawnictwo DSWE, Wrocław 2012.
4. Chacón Delgado P.J., *El concepto de independencia Vasca en Sabino Arana Goiri*, Historia Contemporanea, nr 50, 2014, s. 75-103.
5. Clark P.R., *The Basque insurgent. ETA, 1952-1980*, University of Wisconsin Press, Madison 1984.
6. Conversi D., 2020. *The Left and nationalism. From the French Revolution to the Anthropocene*, [w:] *Research Handbook on Nationalism*, red. L. Greenfeld, Z. Wu, Edward Elgar, Northampton 2020.
7. Conversi D., Espiau G., 2019. *Basque*, [w:] *Comparing Peace Processes*, A. Ozerdem, R. Mac Ginty, Routledge, Londyn, Nowy Jork 2019.
8. Conversi D., *Sovereignty, boundaries and violence. Constructing the Basque national self (1959-2011)*, [w:] *Sovereignty Revisited. The Basque case*, red. I. Güell, P. Åshild, Kolås Åshild, Routledge, Londyn 2017.
9. Darby R., 1994. *Legitimate Targets. A Control or Violence?*, [w:] *New Perspectives on the Nothern Ireland Conflict*, red. A. Guelke, Avebury, Aldershot 1994.
10. De Pablo S., 2000. *El nacionalismo vasco ante el Estado español (1895-1937)*, Studia historica. Historia contemporánea, nr 18, 2000, s. 79-93.
11. EU measures to prevent radicalisation; https://www.consilium.europa.eu/en/policies/preventing-radicalisation/.
12. Garmendia, J.M., *Historia de ETA*, Haranburu, San Sebastian 1979.
13. Global Terrorism Database, https://www.start.umd.edu/gtd/.
14. Górski E., *O demokracji w Hiszpanii (1975-1995)*, Wydawnictwo Instytutu Filozofii i Socjologii PAN, Warszawa 1997.
15. Grotowicz, V., *Terroryzm w Europie Zachodniej*, Wydawnictwo Naukowe PWN, Warszawa 2000.
16. *Hiszpania: ETA ujawniła łączny bilans swoich zamachów*, „Gazeta Prawna", 06.11.2018, https://www.gazetaprawna.pl/wiadomosci/artykuly/1336508,eta-o-liczbie-zamachow.html.
17. Hobsbawm E., *Narody i nacjonalizm po 1870 roku. Program, mit i rzeczywistość*, Wydawnictwo Difin, Warszawa 2010.
18. Informacje dot. procesu radykalizacji; https://tpcoe.gov.pl/cpt/materialy/1799,Informacje-dot-procesu-radykalizacji.html.

19. Jeram S., Conversi D., *Deliberation and Democracy at the End of Armed Conflict. Post-Conflict Opportunities in the Basque Country*, [w:] *Democratic Deliberation in Deeply Divided Societies. From Conflict to Common Ground*, red. J. Ugarizza, D. Clauwaerts, Palgrave Macmillan, Basingstoke 2014.
20. Krutwig F., *Vasconia*, Norbait, Buenos Aires 1973.
21. Kuczyński M., *Krwawiąca Europa. Konflikty zbrojne i punkty zapalne w latach 1990-2000. Tło historyczne i stan obecny*, Bellona, Warszawa 2001.
22. Letamendia Belzunde F., *Historia de Euskadi. El nacionalismo vasco y ETA*, Ruedo Iberico, Paryż 1975.
23. Llanos-Antczak A., *Separatyzm baskijski. Historia, współczesność, perspektywy*, Dom Wydawniczy Elipsa, Warszawa 2019.
24. Miłkowski T., Machcewicz P., *Historia Hiszpanii*, Zakład Narodowy Imienia Ossolińskich, Wrocław 2009.
25. Mirgos K., *Obcy i nowi Baskowie. Migracje, tożsamość i języki w Baskijskiej Wspólnocie Autonomicznej*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2018.
26. Muro D., *What does Radicalisation Look Like? Four Visualisations of Socialisation into Violent Extremism*, Notes Internacionals CIDOB, 2016; https://www.cidob.org/en/publications/what-does-radicalisation-look-four-visualisations-socialisation-violent-extremism.
27. Orzechowska-Wacławska J., *Baskowie. Powstanie współczesnego narodu*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014.
28. Rapaport D.C., *The Four Waves of Modern Terrorism*, [w:] *Attacking Terrorism Elements of a Grand Strategy*, red. A. K. Cronin, J. M. Ludes, Georgetown University Press, Waszyngton 2004.
29. Solozábal Echavarria J.J., *El primer nacionalismo vasco. Industrialismo y conciencia nacional*, Tucar Ediciones, Madryt 1975.
30. Sroka A., *Hiszpańska droga do federalizmu*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2008.
31. Szkurłat I., *Terroryzm a polityka bezpieczeństwa państw Europy Zachodniej na przełomie XX i XXI wieku*, Wydawnictwo Naukowe Akademii Pomorskiej w Słupsku, Słupsk 2018.
32. Szymankiewicz Ł., *The modus operandi of terrorist attacks using improvised explosive devices in landside zones from 2001-2018*, Journal of KONBiN, vol. 52, iss. 3, 2022, s. 123-135.
33. Terradillos A., *ETA anuncia su disolución*, Ser, 03.05.2018; https://cadenaser.com/ser/2018/05/03/politica/1525346984_523675.html.
34. *Una nueva interpretacion de la historia de Bizkaia*, http://www.sabinetxea.org/libro/libro/libro.html.

dr Iwona Lasek-Surowiec
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0002-7231-7993

dr Bartosz Błaszczak
Wyższa Szkoła Kształcenia Zawodowego we Wrocławiu
ORCID-0009-0002-0457-4434

dr Irena Malinowska
Wyższa Szkoła Kształcenia Zawodowego we Wrocławiu
ORCID: 0000-0002-9194-3121

dr Marcin Oskierko
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0003-3450-6037
https://doi.org/10.29316/9788368103199_4

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO I AGENCJA WYWIADU W ZWALCZANIU TERRORYZMU NA POZIOMIE KRAJOWYM I MIĘDZYNARODOWYM

INTERNAL SECURITY AGENCY AND INTELLIGENCE AGENCY IN COUNTER-TERRORISM AT NATIONAL AND INTERNATIONAL LEVEL

Streszczenie

Celem niniejszego rozdziału jest analiza roli Agencji Bezpieczeństwa Wewnętrznego (ABW) i Agencji Wywiadu (AW)

Summary

The aim of this chapter is to analyze the role of the Internal Security Agency (ABW) and the Foreign Intelligence Agency (AW) in

w zwalczaniu terroryzmu, ze szczególnym uwzględnieniem ich kompetencji, metod działania oraz współpracy międzynarodowej. W pierwszej części przedstawiono charakterystykę współczesnych zagrożeń terrorystycznych, koncentrując się na ich ewolucji, metodach działania organizacji terrorystycznych oraz nowych wyzwaniach, takich jak cyberterroryzm i ataki asymetryczne. Druga część rozdziału opisuje funkcjonowanie ABW i AW w systemie bezpieczeństwa narodowego, omawiając ich zakres kompetencji, działania operacyjne oraz kluczowe zadania związane z przeciwdziałaniem terroryzmowi. Trzecia część poświęcona jest międzynarodowej współpracy w zwalczaniu terroryzmu, przedstawiając zaangażowanie Polski w struktury bezpieczeństwa NATO, Unii Europejskiej, Interpolu oraz współpracę bilateralną z innymi państwami. Główny problem badawczy sformułowano: Jakie są najskuteczniejsze metody stosowane przez ABW i AW w zwalczaniu terroryzmu międzynarodowego oraz jakie wyzwania stoją przed tymi instytucjami w obliczu zmieniających się zagrożeń? Hipoteza badawcza zakłada, że skuteczność działań ABW i AW w zwalczaniu terroryzmu zależy od ich zdolności do integracji nowoczesnych technologii, międzynarodowej współpracy oraz elastycznego dostosowywania strategii do nowych form zagrożeń. W rozdziale zastosowano metody teoretyczne, takie jak analiza literatury przedmiotu, aktów prawnych oraz raportów instytucji zajmujących się bezpieczeństwem międzynarodowym. Dzięki tym metodom możliwe było przeprowadzenie kompleksowej analizy skuteczności działań ABW i AW oraz sformułowanie wniosków dotyczących przyszłych kierunków ich rozwoju.

Słowa kluczowe: terroryzm międzynarodowy, bezpieczeństwo narodowe, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, współpraca międzynarodowa

combating terrorism, with particular emphasis on their competences, methods of operation and international cooperation. The first part presents the characteristics of contemporary terrorist threats, focusing on their evolution, the methods of operation of terrorist organizations and new challenges, such as cyberterrorism and asymmetric attacks. The second part of the chapter describes the functioning of the Internal Security Agency and the Internal Security Agency in the national security system, discussing their scope of competences, operational activities and key tasks related to counteracting terrorism. The third part is devoted to international cooperation in combating terrorism, presenting Polish's involvement in the security structures of NATO, the European Union, Interpol and bilateral cooperation with other countries. The main research problem was formulated: What are the most effective methods used by the Internal Security Agency and the Internal Security Agency in combating international terrorism and what challenges do these institutions face in the face of changing threats? The research hypothesis assumes that the effectiveness of the activities of the Internal Security Agency and the Armed Forces in combating terrorism depends on their ability to integrate modern technologies, international cooperation and flexible adaptation of strategies to new forms of threats. The chapter uses theoretical methods, such as the analysis of the literature on the subject, legal acts and reports of institutions dealing with international security. Thanks to these methods, it was possible to carry out a comprehensive analysis of the effectiveness of the activities of the Internal Security Agency and the Internal Security Agency and to formulate conclusions regarding the future directions of their development.

Keywords: international terrorism, national security, Internal Security Agency, Foreign Intelligence Agency, international cooperation

Wstęp

Współczesne zagrożenia terrorystyczne stanowią jedno z największych wyzwań dla bezpieczeństwa państw na całym świecie. Dynamiczny rozwój technologii, globalizacja oraz migracje sprzyjają rozwojowi międzynarodowych sieci terrorystycznych, które wykorzystują nowe metody działania, w tym cyberterroryzm, propagandę w mediach społecznościowych oraz ataki asymetryczne. W odpowiedzi na te zagrożenia, państwa podejmują działania prewencyjne i operacyjne, angażując wyspecjalizowane służby bezpieczeństwa.

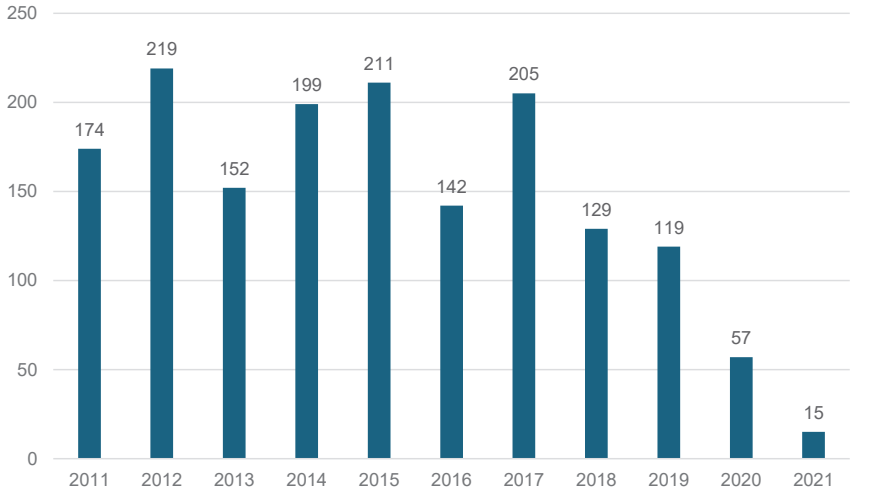
W Polsce kluczową rolę w zwalczaniu terroryzmu odgrywają Agencja Bezpieczeństwa Wewnętrznego (ABW) oraz Agencja Wywiadu (AW). Pierwsza z nich koncentruje się na wykrywaniu, zapobieganiu i neutralizacji zagrożeń terrorystycznych wewnątrz kraju, natomiast AW działa na arenie międzynarodowej, dostarczając kluczowych informacji wywiadowczych dotyczących potencjalnych zagrożeń. Współpraca obu agencji, zarówno na poziomie krajowym, jak i międzynarodowym, jest niezbędna do skutecznego przeciwdziałania terroryzmowi oraz zapewnienia bezpieczeństwa obywatelom.

Celem niniejszego rozdziału jest analiza roli ABW i AW w zwalczaniu terroryzmu międzynarodowego, ze szczególnym uwzględnieniem ich kompetencji, metod działania oraz współpracy z partnerami zagranicznymi. Przedstawiona zostanie także ewolucja działań antyterrorystycznych w Polsce w kontekście zmieniających się zagrożeń globalnych oraz analiza skuteczności podjętych strategii.

Współczesne zagrożenia terrorystyczne

Terroryzm międzynarodowy stanowi jedno z największych wyzwań dla współczesnych państw i organizacji międzynarodowych, wpływając zarówno na bezpieczeństwo wewnętrzne, jak i geopolityczną stabilność świata. W ostatnich dekadach obserwujemy dynamiczną ewolucję zagrożeń terrorystycznych, które nie ograniczają się już wyłącznie do tradycyjnych ataków fizycznych, ale obejmują także działania w cyberprzestrzeni, dezinformację oraz różnego rodzaju ataki asymetryczne. Zgodnie ze sprawozdaniem dotyczącym sytuacji i tendencji w dziedzinie terroryzmu w Unii Europejskiej (TE-SAT) z 2024 r., w 2023 r. w UE odnotowano 120 ataków terrorystycznych, w tym 98 przeprowadzonych skutecznie, 9 nieudanych i 13 udaremnionych. To gwałtowny wzrost w porównaniu

z 2022 r., kiedy było to 28 ataków i z 2021 r, gdy było 18 ataków[1]. Poniżej na rysunku przedstawiono liczbę ataków terrorystycznych za lata 2010-2021.



Rysunek 1. Liczba ataków terrorystycznych za lata 2010-2021

Źródło: *Terroryzm w UE: fakty i liczby*, Consilium, https://www.consilium.europa.eu/pl/infographics/terrorism-eu-facts-figures/#0, [dostęp: 10.03.2025].

Za najwięcej ataków przeprowadzonych skutecznie (70) odpowiadają grupy separatystyczne. Ugrupowania dżihadystyczne przeprowadziły pięć zamachów, w których zginęło 12 osób, a 6 zostało rannych.

Działalność organizacji terrorystycznych ewoluowała wraz z postępem technologicznym oraz procesami globalizacyjnymi[2]. Współczesny terroryzm nie ogranicza się już wyłącznie do działań prowadzonych przez scentralizowane grupy, ale coraz częściej przybiera formę tzw. terroryzmu rozproszonego, w którym aktywne są niewielkie komórki lub samotne wilki, działające w oparciu o ideologię inspirowaną przez większe organizacje, takie jak Al-Kaida, Państwo Islamskie (ISIS) czy różne ugrupowania skrajnie prawicowe

[1] *Terroryzm w UE: ataki, ofiary śmiertelne i zatrzymania w 2023 r.*, Parlament Europejski, https://www.europarl.europa.eu/topics/pl/article/20250124STO26468/terroryzm-w-ue-ataki-ofiary-smiertelne-i-zatrzymania-w-2023-r, [dostęp: 10.03.2025].

[2] E. Kacperska, *Terroryzm międzynarodowy jako problem globalny współczesnej gospodarki*, Zeszyty Naukowe Szkoły Głównej Gospodarstwa Wiejskiego. Ekonomika i Organizacja Gospodarki Żywnościowej, nr 120, 2017, s. 17.

i lewicowe[3]. Współcześnie uznaje się, że terroryzm najlepiej charakteryzują jego konkretne przejawy, które obejmują różne formy bezprawnych działań o charakterze terrorystycznym. Do najczęściej spotykanych należą:

- przejmowanie środków transportu, takich jak pojazdy lądowe, statki czy samoloty, w celu uprowadzenia pasażerów i wykorzystania ich jako zakładników,
- działania sabotażowe skierowane przeciwko sektorowi gospodarczemu, mające na celu destabilizację ekonomiczną,
- przestępczość pospolita, obejmująca m.in. rozboje, kradzieże i włamania, które służą jako źródło finansowania grup terrorystycznych,
- zamachy na osoby sprawujące władzę, przedstawicieli kluczowych sektorów gospodarki oraz osoby objęte ochroną międzynarodową,
- porwania cudzoziemców i bezprawne przetrzymywanie ich w celu uzyskania okupu lub realizacji innych celów politycznych,
- ataki z użyciem materiałów wybuchowych, broni palnej czy rakiet w przestrzeni publicznej, stwarzające zagrożenie dla przypadkowych osób,
- zastosowanie substancji chemicznych, biologicznych, radioaktywnych lub trujących w celu skażenia określonych obszarów lub środków transportu publicznego, prowadzące do zagrożenia zdrowia i życia ludności[4].

Każde z tych działań stanowi istotne zagrożenie dla bezpieczeństwa narodowego i międzynarodowego, przyczyniając się do destabilizacji porządku publicznego oraz wywoływania strachu w społeczeństwie.

Szczególnym wyzwaniem jest wykorzystywanie przez terrorystów nowoczesnych technologii. Media społecznościowe oraz komunikatory szyfrowane stały się kluczowym narzędziem rekrutacji, propagandy i koordynacji działań. Przykładem może być Państwo Islamskie, które w szczytowym okresie swojej aktywności intensywnie wykorzystywało platformy takie jak Twitter, Telegram czy Facebook do szerzenia propagandy, rekrutacji bojowników oraz organizowania ataków na całym świecie[5]. W ten sposób granice geograficzne przestały stanowić przeszkodę w działalności terrorystycznej, a organizacje te zyskały zdolność do inspirowania zamachów nawet w krajach, które

[3] K. Wardin, *Al -Kaida Internacjonalizacja terroryzmu samobójczego*, Rocznik Bezpieczeństwa Międzynarodowego, nr 2, 2019, s. 179.

[4] L. Goździewski, *Terroryzm jako zjawisko społeczne i zagrożenie światowego bezpieczeństwa*, Journal of Modern Science, nr 44(1), 2020, s. 210-211.

[5] B. Hałas, *Promocja terroryzmu w Internecie i przeciwdziałanie ze strony Unii Europejskiej*, Przegląd Geopolityczny, 40, 2022, s. 122.

nie były ich bezpośrednim celem. Można przyjąć, że media społecznościowe spełniają dla terrorystów dwie funkcje:

- informacyjno-propagandowe;
- taktyczno-operacyjne[6].

Media społecznościowe stały się potężnym narzędziem wykorzystywanym przez organizacje terrorystyczne do szerzenia ideologii, rekrutacji, finansowania oraz koordynowania działań. Dynamiczny rozwój technologii sprawia, że walka z terroryzmem w sieci staje się coraz większym wyzwaniem dla służb bezpieczeństwa na całym świecie. Dlatego też państwa i organizacje międzynarodowe nieustannie poszukują nowych metod monitorowania i eliminowania treści ekstremistycznych, jednocześnie dbając o ochronę wolności słowa i prywatności użytkowników Internetu.

Jednym z najnowszych i najbardziej niebezpiecznych obliczy współczesnego terroryzmu również związanym z postępem technologicznym jest cyberterroryzm. Cyberterroryzm jest formą terroryzmu polegającą generalnie na wykorzystaniu komputerów i systemów informatycznych jako podstawowego narzędzia przestępczego lub uczynienia z nich głównego celu tychże działań[7].

Wraz z rozwojem infrastruktury cyfrowej i rosnącą zależnością społeczeństw od technologii informatycznych, organizacje terrorystyczne zaczęły wykorzystywać cyberprzestrzeń nie tylko do komunikacji i propagandy, ale także do przeprowadzania ataków na krytyczną infrastrukturę państw[8]. Cyberterroryzm obejmuje działania takie jak:

- ataki na infrastrukturę krytyczną – próby zakłócenia pracy sieci energetycznych, systemów wodociągowych czy sieci transportowych, co może prowadzić do paraliżu gospodarki i chaosu społecznego;
- ataki na systemy finansowe – przejęcie kontroli nad systemami bankowymi lub kradzież środków finansowych w celu finansowania działalności terrorystycznej;

[6] G. Libora, *Oblicza współczesnego terroryzmu.* Wydanie I, Wydawnictwo internetowe e-bookowo, 2016, s. 46.

[7] J. Gerwatowski, *Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego*, Kwartalnik Studia Prawnoustrojowe 2019, nr 44, s. 92.

[8] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Zeszyty Naukowe Akademii Marynarki Wojennej, nr 1(160), 2005, s. 174.

- dezinformacja i propaganda – szerzenie fałszywych informacji w sieci w celu destabilizacji społeczeństw, wzbudzania paniki oraz manipulowania opinią publiczną.

Zagrożenie cyberterrorystyczne stało się na tyle poważne, że coraz więcej państw inwestuje w rozwój wyspecjalizowanych jednostek do walki z tego typu atakami. Równie ważna w tej sytuacji jest efektywna współpraca pomiędzy państwami i organizacjami międzynarodowymi oraz tworzenie odpowiednich narzędzi[9]. Przykładem jest utworzenie specjalnych centrów cyberbezpieczeństwa w NATO (NATO Cyber Security Centre) oraz Unii Europejskiej (EU Cyber Defence Coordination Centre), które zajmują się monitorowaniem i przeciwdziałaniem zagrożeniom.

Procesy globalizacyjne oraz masowe migracje, zwłaszcza te wynikające z konfliktów zbrojnych na Bliskim Wschodzie i w Afryce Północnej, wpłynęły na rozprzestrzenianie się ideologii ekstremistycznych w różnych częściach świata. Niektóre państwa europejskie doświadczyły problemów związanych z radykalizacją części społeczności migrantów, zwłaszcza w kontekście trudnej integracji oraz marginalizacji społecznej.

Z drugiej strony, należy podkreślić, że problem ten jest złożony i nie można go jednoznacznie przypisać migracjom jako całości. Radykalizacja może mieć wiele źródeł, w tym działalność ekstremistycznych duchownych, internetową propagandę czy osobiste doświadczenia jednostek związane z konfliktami zbrojnymi.

W odpowiedzi na rosnące zagrożenie terroryzmem międzynarodowym, państwa wzmacniają swoje systemy bezpieczeństwa i wywiadu. Działania te obejmują m.in.:

- rozwój technologii monitoringu i analizy danych – wykorzystanie sztucznej inteligencji do wykrywania zagrożeń w cyberprzestrzeni;
- zaostrzenie polityki antyterrorystycznej – wprowadzenie surowszych przepisów dotyczących działalności podejrzanych grup i osób, np. poprzez penalizację propagandy terrorystycznej w Internecie;
- wzmożona współpraca międzynarodowa – wymiana informacji wywiadowczych między krajami UE, NATO i innymi organizacjami zajmującymi się zwalczaniem terroryzmu.

[9] J. Gerwatowski, *Cyberterroryzm jako efekt rozwoju nowych technologii informatycznych w pierwszej i drugiej dekadzie XXI wieku*, Przegląd Policyjny, nr 1(141), 2021, s. 290.

Współczesne zagrożenia terrorystyczne są wielowymiarowe i dynamiczne, a ich zwalczanie wymaga kompleksowego podejścia obejmującego działania operacyjne, prewencyjne oraz technologiczne. Państwa na całym świecie, w tym Polska, dostosowują swoje strategie do nowych form zagrożeń, koncentrując się na współpracy międzynarodowej, monitorowaniu cyberprzestrzeni oraz rozwoju nowoczesnych narzędzi do wykrywania i neutralizacji zagrożeń terrorystycznych[10].

W kontekście Polski kluczową rolę w zwalczaniu terroryzmu odgrywają Agencja Bezpieczeństwa Wewnętrznego (ABW) oraz Agencja Wywiadu (AW), które monitorują zagrożenia wewnętrzne i zewnętrzne, analizują potencjalne ryzyka i współpracują z partnerami międzynarodowymi w zakresie przeciwdziałania terroryzmowi.

Rola ABW i AW w systemie bezpieczeństwa

W Polsce zwalczanie terroryzmu jest jednym z kluczowych elementów systemu bezpieczeństwa narodowego. Zadania te realizują przede wszystkim Agencja Bezpieczeństwa Wewnętrznego (ABW) oraz Agencja Wywiadu (AW), które współpracują zarówno na poziomie krajowym, jak i międzynarodowym. Każda z tych instytucji pełni odrębne, ale komplementarne funkcje, dzięki czemu system przeciwdziałania zagrożeniom terrorystycznym jest wielopoziomowy i skutecznie dostosowany do aktualnych wyzwań.

ABW jest główną instytucją odpowiedzialną za zapewnienie bezpieczeństwa wewnętrznego państwa oraz zwalczanie terroryzmu na terytorium Polski. Jej zadania obejmują zarówno działania operacyjne, jak i analityczno-śledcze, mające na celu wykrywanie, zapobieganie oraz neutralizację zagrożeń. Do głównych zadań ABW w zakresie przeciwdziałania terroryzmowi należą:

- monitorowanie zagrożeń terrorystycznych – identyfikacja i analiza potencjalnych zagrożeń związanych z działalnością grup ekstremistycznych, zarówno rodzimych, jak i zagranicznych;
- działania operacyjne i rozpoznawcze – wykrywanie osób powiązanych z organizacjami terrorystycznymi, przeciwdziałanie radykalizacji oraz neutralizacja podejrzanych działań;

[10] D. Brążkiewicz, S. Żurawski, Z. Ciekanowski, P. Ochyra, *Udział Sił Zbrojnych RP w zwalczaniu terroryzmu*, Studia Administracji i Bezpieczeństwa, 16(16), Gorzów Wielkopolski 2024, s. 197.

- rozpracowywanie finansowania terroryzmu – śledzenie przepływów finansowych, eliminacja kanałów finansowania grup terrorystycznych oraz współpraca z instytucjami bankowymi w zakresie przeciwdziałania praniu brudnych pieniędzy.
- współpraca z innymi służbami – koordynacja działań z Policją, Strażą Graniczną, Żandarmerią Wojskową oraz innymi instytucjami odpowiedzialnymi za bezpieczeństwo;
- zapobieganie cyberterroryzmowi – wykrywanie i neutralizowanie zagrożeń w cyberprzestrzeni, m.in. ataków na infrastrukturę krytyczną, szerzenia propagandy terrorystycznej oraz prób rekrutacji przez Internet;
- ochrona infrastruktury krytycznej – analiza potencjalnych zagrożeń i wdrażanie mechanizmów zabezpieczających kluczowe obiekty państwowe, energetyczne, transportowe i telekomunikacyjne przed możliwymi atakami;
- współpraca międzynarodowa – wymiana informacji z partnerami zagranicznymi, w tym Europolem, INTERPOL-em oraz służbami bezpieczeństwa innych państw.

ABW działa zarówno w sposób jawny, np. wydając ostrzeżenia o zagrożeniach i raporty analityczne, jak i w trybie operacyjnym, prowadząc tajne śledztwa i akcje antyterrorystyczne.

Ustawa o ABW oraz AW dookreśliła, że zadania ABW wskazane w art. 5, w tym te nakierowane na zwalczanie terroryzmu, są realizowane poprzez wykonywanie przez funkcjonariuszy ABW:

1) na poziomie identyfikacji i eliminacji zagrożeń – czynności operacyjno-rozpoznawczych i analityczno-informacyjnych w celu pozyskiwania i przetwarzania informacji istotnych dla ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego;
2) na poziomie zwalczania przestępstw – czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych w celu rozpoznawania, wykrywania przestępstw i zapobiegania im oraz ścigania ich sprawców[11].

Wybór Szefa ABW na koordynatora działań organów ścigania karnego w fazie zapobiegania zdarzeniom terrorystycznym wydaje się oczywisty, przede wszystkim w świetle przepisów kompetencyjnych ABW, doświadczeń, jakie ma ta służba oraz jej zdolności organizacyjnych w tym obszarze, związanych

[11] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2002 Nr 74, poz. 676), art. 21 ust. 1.

głównie z jednostkami funkcjonującymi w jej strukturze – Centrum Antyterrorystycznym (CAT) oraz Centrum Prewencji Terrorystycznej (CPT)[12].

Z kolei Agencja Wywiadu (AW) koncentruje się na zdobywaniu i analizie informacji wywiadowczych poza granicami kraju, co ma kluczowe znaczenie dla ochrony Polski przed zagrożeniami o charakterze międzynarodowym. Najważniejsze zadania AW w zakresie zwalczania terroryzmu obejmują:

- zbieranie danych o organizacjach terrorystycznych – identyfikacja grup terrorystycznych operujących na arenie międzynarodowej i ich potencjalnych powiązań z Polską;
- rozpracowywanie międzynarodowych sieci terrorystycznych – śledzenie działalności ekstremistycznych grup, ich struktur organizacyjnych oraz metod działania;
- monitorowanie zagrożeń globalnych – analiza sytuacji politycznej w regionach szczególnie narażonych na działalność terrorystyczną, takich jak Bliski Wschód, Afryka Północna czy Azja Południowa;
- zapobieganie przemytowi broni i materiałów wybuchowych – identyfikacja międzynarodowych szlaków przemytu, które mogą być wykorzystywane przez grupy terrorystyczne do przeprowadzania zamachów;
- współpraca z zagranicznymi służbami wywiadowczymi – wymiana informacji z wywiadem państw sojuszniczych (m.in. NATO, UE, USA), co umożliwia skuteczne wykrywanie zagrożeń, jeszcze przed ich dotarciem do Polski;
- identyfikacja zagranicznych bojowników – śledzenie działań obywateli Polski, którzy mogli zostać zradykalizowani i dołączyć do międzynarodowych organizacji terrorystycznych;
- operacje specjalne – prowadzenie działań mających na celu eliminację zagrożeń poza granicami Polski, np. poprzez infiltrację grup terrorystycznych lub zdobywanie kluczowych informacji dotyczących planowanych ataków.

AW działa głównie w sferze tajnych operacji wywiadowczych, co oznacza, że jej skuteczność często pozostaje poza wiedzą opinii publicznej. Współpraca z innymi agencjami wywiadowczymi oraz stałe monitorowanie sytuacji międzynarodowej pozwala Polsce skutecznie reagować na potencjalne zagrożenia.

[12] P. Burczaniuk, *Zadania i uprawnienia organów ścigania karnego w zakresie zwalczania terroryzmu w Polsce – perspektywa prawna*, Terroryzm. Studia, analizy, prewencja, 2(2), 2022, s. 13.

ABW i AW, choć pełnią różne role w systemie bezpieczeństwa, muszą ściśle współpracować w celu skutecznego zwalczania terroryzmu. Ich współdziałanie obejmuje m.in.:

- wymianę informacji dotyczących zagrożeń wewnętrznych i zewnętrznych,
- wspólne operacje śledcze i wywiadowcze,
- analizowanie potencjalnych powiązań między krajowymi a zagranicznymi komórkami terrorystycznymi,
- współpracę w zakresie ochrony granic przed przenikaniem terrorystów i ich zwolenników do Polski,
- koordynację działań w ramach organizacji międzynarodowych (NATO, UE, INTERPOL).

Dzięki tej współpracy możliwe jest skuteczniejsze wykrywanie i eliminowanie zagrożeń terrorystycznych na różnych poziomach – zarówno wewnątrz kraju, jak i poza jego granicami.

Agencja Bezpieczeństwa Wewnętrznego (ABW) oraz Agencja Wywiadu (AW) stanowią filary polskiego systemu ochrony przed terroryzmem. Podczas gdy ABW koncentruje się na działaniach krajowych, monitorując i neutralizując zagrożenia wewnętrzne, AW operuje na arenie międzynarodowej, zbierając informacje wywiadowcze i analizując działania grup terrorystycznych poza Polską. Współpraca obu służb oraz ich kooperacja z partnerami zagranicznymi są kluczowe dla zapewnienia bezpieczeństwa narodowego oraz skutecznej walki z międzynarodowym terroryzmem.

Współpraca międzynarodowa w zwalczaniu terroryzmu

Terroryzm stanowi jedno z najpoważniejszych zagrożeń o charakterze globalnym, dlatego jego skuteczne zwalczanie wymaga ścisłej współpracy między państwami. Organizacje terrorystyczne działają ponad granicami, wykorzystując nowoczesne technologie oraz międzynarodowe szlaki komunikacyjne i finansowe. W związku z tym Agencja Bezpieczeństwa Wewnętrznego (ABW) i Agencja Wywiadu (AW) aktywnie uczestniczą w międzynarodowej kooperacji w zakresie wymiany informacji wywiadowczych, wspólnych operacji oraz działań profilaktycznych.

Polska jako członek Unii Europejskiej, współpracuje z różnymi instytucjami unijnymi zajmującymi się bezpieczeństwem, takimi jak Europejskie

Centrum ds. Zwalczania Terroryzmu (ECTC), działające w ramach Europolu[13]. Dzięki temu ABW i AW mogą skutecznie identyfikować osoby i grupy podejrzewane o działalność terrorystyczną oraz monitorować potencjalne zagrożenia. Współpraca ta obejmuje również wymianę informacji z Europejską Służbą Działań Zewnętrznych oraz Europejską Agencją ds. Współpracy Organów Ścigania, co umożliwia lepszą koordynację działań w całej Europie. Dodatkowo, Polska uczestniczy w systemie Schengen Information System (SIS), który pozwala na monitorowanie osób podejrzanych o związki z terroryzmem w obrębie strefy Schengen.

Poza Unią Europejską Polska współpracuje z NATO, co ma kluczowe znaczenie dla globalnego bezpieczeństwa. ABW i AW biorą udział w działaniach prowadzonych przez NATO Counter-Terrorism Unit oraz w programach monitorowania zagrożeń pochodzących z Bliskiego Wschodu i Afryki Północnej[14]. Agencja Wywiadu uczestniczy w wymianie informacji w ramach NATO Intelligence Fusion Centre, dzięki czemu możliwe jest lepsze rozpoznanie globalnych struktur terrorystycznych i przeciwdziałanie im na wczesnym etapie.

Kolejnym ważnym obszarem współpracy są działania prowadzone w ramach Interpolu i Europolu. Polska regularnie wymienia informacje na temat podejrzanych osób, nielegalnego finansowania terroryzmu oraz transgranicznych szlaków przerzutowych broni i materiałów wybuchowych. Dzięki temu możliwe jest skuteczniejsze zapobieganie zagrożeniom i neutralizowanie siatek terrorystycznych działających na terenie Europy[15]. Ponadto, Polska angażuje się w programy zwalczania zagranicznych bojowników, koncentrując się na identyfikacji osób powracających z obszarów konfliktów, które mogły zostać zradykalizowane.

Na arenie globalnej Polska współpracuje z Organizacją Narodów Zjednoczonych, wspierając Global Counter-Terrorism Strategy, której celem jest ograniczenie finansowania terroryzmu oraz przeciwdziałanie radykalizacji. Globalna strategia antyterrorystyczna Organizacji Narodów Zjednoczonych

[13] M. Łuczkowska, *Działaniu Unii Europejskiej w zakresie zwalczania terroryzmu*, Rocznik Bezpieczeństwa Międzynarodowego, vol. 10, nr 2, 2016, s. 131.

[14] Działania antyterrorystyczne Sojuszu Północnoatlantyckiego NATO - Aktualności Wydział Prewencji Zagrożeń CAT ABW, https://tpcoe.gov.pl/cpt/aktualnosci/1910,Dzialania-antyterrorystyczne-Sojuszu-Polnocnoatlantyckiego-NATO.html, [dostęp: 10.03.2025].

[15] K. Sobowiec, *Terroryzm jako jedno z największych zagrożeń bezpieczeństwa współczesnego świata,* [w:] *Budowanie poczucia bezpieczeństwa w czasach pandemii oraz zagrożenia terroryzmem i wojną*, red. E. Jasiuk, A. Chochowska, Oficyna Wydawnicza Uczelni Łazarskiego, Warszawa 2023, s. 186.

w formie rezolucji i załączonego do niej planu działania (A/RES/60/288) składa się z czterech filarów, a mianowicie:

- Środki mające na celu zaradzenie warunkom sprzyjającym rozprzestrzenianiu się terroryzmu.
- Środki mające na celu zapobieganie terroryzmowi i jego zwalczanie.
- Środki mające na celu budowanie zdolności państw do zapobiegania terroryzmowi i zwalczania go oraz wzmocnienie roli systemu Narodów Zjednoczonych w tym zakresie.
- Środki mające na celu zapewnienie poszanowania praw człowieka dla wszystkich i praworządności jako podstawy walki z terroryzmem[16].

W ramach ONZ Polska wdraża również postanowienia Rady Bezpieczeństwa dotyczące zwalczania terroryzmu, w tym rezolucję 1373, zobowiązującą państwa członkowskie do podejmowania działań legislacyjnych na rzecz przeciwdziałania działalności terrorystycznej.

Obok współpracy wielostronnej Polska prowadzi także ścisłą współpracę bilateralną z kluczowymi partnerami. Relacje z USA obejmują kooperację z Federalnym Biurem Śledczym (FBI) oraz Centralną Agencją Wywiadowczą (CIA), co pozwala na skuteczniejsze monitorowanie globalnych zagrożeń i przeciwdziałanie ekstremizmowi[17]. Polska bierze również udział w wspólnych operacjach związanych z cyberbezpieczeństwem oraz analizą przepływów finansowych wykorzystywanych przez organizacje terrorystyczne. Dodatkowo, współpraca z Izraelem umożliwia wymianę doświadczeń w zakresie operacji antyterrorystycznych i ochrony infrastruktury krytycznej.

W ramach współpracy europejskiej Polska utrzymuje bliskie kontakty z Niemcami, Francją oraz Wielką Brytanią, koncentrując się na wymianie informacji o zagrożeniach terrorystycznych oraz wspólnych działaniach mających na celu zwalczanie siatek przestępczych. Współpraca ta obejmuje również kontrolę granic i przeciwdziałanie nielegalnej migracji, która w niektórych przypadkach może być wykorzystywana przez terrorystów do przenikania na teren Europy.

[16] Globalna strategia antyterrorystyczna Organizacji Narodów Zjednoczonych, Urząd ds. Zwalczania Terroryzmu, https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy, [dostęp: 10.03.2025].

[17] Dyrektor CIA w Polsce - Służby specjalne, Portal Gov.pl, https://www.gov.pl/web/sluzby-specjalne/dyrektor-cia-w-polsce, [dostęp: 10.03.2025].

Pomimo rosnącej współpracy międzynarodowej Polska i inne kraje napotykają liczne wyzwania w walce z terroryzmem[18]. Jednym z najpoważniejszych problemów jest brak jednolitej polityki antyterrorystycznej w Unii Europejskiej, co utrudnia skoordynowane działania. Ponadto, organizacje terrorystyczne coraz częściej korzystają z zaszyfrowanej komunikacji, co znacząco utrudnia monitorowanie ich działań. Innym wyzwaniem jest śledzenie przepływów finansowych, zwłaszcza w kontekście wykorzystywania kryptowalut do finansowania działalności terrorystycznej. Dodatkowo, wiele państw boryka się z problemem zagranicznych bojowników, czyli osób powracających z obszarów konfliktów zbrojnych, które mogą stanowić potencjalne zagrożenie dla bezpieczeństwa wewnętrznego.

Aby skuteczniej przeciwdziałać terroryzmowi na arenie międzynarodowej, Polska powinna dążyć do usprawnienia wymiany informacji wywiadowczych oraz intensyfikacji współpracy technologicznej. Rozwój narzędzi analizy danych oraz wykorzystanie sztucznej inteligencji w identyfikowaniu potencjalnych zagrożeń mogą znacząco zwiększyć skuteczność działań służb bezpieczeństwa. Równie istotne jest wzmacnianie zdolności w zakresie cyberbezpieczeństwa, zwłaszcza w kontekście rosnącej aktywności terrorystów w Internecie. Ponadto, przyszłość walki z terroryzmem będzie wymagać lepszej koordynacji operacji antyterrorystycznych na poziomie globalnym, tak aby eliminować zagrożenia już na wczesnym etapie ich planowania.

Współpraca międzynarodowa stanowi kluczowy element skutecznej walki z terroryzmem, a Polska, poprzez ABW i AW, aktywnie uczestniczy w strukturach zajmujących się zwalczaniem zagrożeń terrorystycznych. Dzięki zaangażowaniu w międzynarodowe działania Polska może skuteczniej monitorować zagrożenia, prowadzić operacje prewencyjne oraz eliminować potencjalne ryzyka związane z działalnością ekstremistyczną. W przyszłości kluczowe znaczenie będzie miało dalsze rozwijanie współpracy technologicznej, wzmacnianie zdolności analitycznych oraz budowanie efektywnych systemów wymiany informacji, co pozwoli na jeszcze skuteczniejsze przeciwdziałanie terroryzmowi.

[18] S. Żurawski, M. Oskierko, *Actions of the Border Guard in the event of a terrorist attack at the airport*, Studia Bezpieczeństwa Narodowego, Zeszyt 32, 2024, s. 78.

Podsumowanie

Walka z terroryzmem jest jednym z najważniejszych wyzwań współczesnych państw, wymagającym wielowymiarowego podejścia i skutecznej współpracy zarówno na poziomie krajowym, jak i międzynarodowym. Analiza działań podejmowanych przez Agencję Bezpieczeństwa Wewnętrznego (ABW) oraz Agencję Wywiadu (AW) pokazuje, że Polska wdrożyła szereg skutecznych mechanizmów przeciwdziałania zagrożeniom terrorystycznym, jednak dynamiczny rozwój technologii oraz zmieniający się charakter zagrożeń wymagają ciągłego doskonalenia strategii.

Mimo podejmowanych działań, zagrożenie terroryzmem nieustannie ewoluuje, przybierając nowe formy, takie jak cyberterroryzm, ataki asymetryczne oraz wykorzystywanie zaawansowanych technologii do radykalizacji i propagandy. Organizacje terrorystyczne coraz częściej wykorzystują Internet i media społecznościowe do rekrutacji nowych członków, finansowania działalności oraz organizowania ataków. Dodatkowo, wyzwania związane z kontrolą transgranicznych przepływów finansowych, migracją i bezpieczeństwem cybernetycznym wymagają nowych, bardziej złożonych mechanizmów ochrony.

Terroryzm pozostaje jednym z największych wyzwań XXI wieku, a jego zwalczanie wymaga ciągłego dostosowywania strategii do dynamicznie zmieniających się realiów. Polska, poprzez działania ABW i AW, skutecznie realizuje politykę bezpieczeństwa, jednak dalsze inwestycje w nowe technologie, edukację społeczną oraz współpracę międzynarodową są niezbędne dla zapewnienia długoterminowej ochrony przed zagrożeniami terrorystycznymi.

Tylko kompleksowe podejście, obejmujące zarówno działania prewencyjne, jak i operacyjne, pozwoli na skuteczną ochronę przed zagrożeniami terrorystycznymi oraz minimalizację ich skutków. Polska powinna kontynuować rozwój nowoczesnych narzędzi analitycznych, wzmacniać swoje zdolności operacyjne i dążyć do jeszcze ściślejszej współpracy na arenie międzynarodowej, aby skutecznie przeciwdziałać terroryzmowi w przyszłości.

Literatura

1. Brążkiewicz D., Żurawski S., Ciekanowski Z., Ochyra P., *Udział Sił Zbrojnych RP w zwalczaniu terroryzmu*, Studia Administracji i Bezpieczeństwa, 16(16), 2024, s. 275-290. https://doi.org/10.5604/01.3001.0054.6438.
2. Burczaniuk P., *Zadania i uprawnienia organów ścigania karnego w zakresie zwalczania terroryzmu w Polsce – perspektywa prawna*, Terroryzm. Studia, analizy, prewencja, 2(2), 2022, s. 9-30. https://doi.org/10.4467/27204383TER.22.017.16337.

3. Dyrektor CIA w Polsce - Służby specjalne, Portal Gov.pl, https://www.gov.pl/web/sluzby-specjalne/dyrektor-cia-w-polsce.
4. Działania antyterrorystyczne Sojuszu Północnoatlantyckiego NATO - Aktualności Wydział Prewencji Zagrożeń CAT ABW, https://tpcoe.gov.pl/cpt/aktualnosci/1910,Dzialania-antyterrorystyczne-Sojuszu-Polnocnoatlantyckiego-NATO.html.
5. Globalna strategia antyterrorystyczna Organizacji Narodów Zjednoczonych, Urząd ds. Zwalczania Terroryzmu, https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy.
6. Gerwatowski J., *Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego*, Kwartalnik Studia Prawnoustrojowe, 44, 2019, s. 89-106. https://doi.org/10.31648/sp.4897.
7. Gerwatowski J., *Cyberterroryzm jako efekt rozwoju nowych technologii informatycznych w pierwszej i drugiej dekadzie XXI wieku*, Przegląd Policyjny, nr 1(141), 2021, s. 269-296.
8. Goździewski L., *Terroryzm jako zjawisko społeczne i zagrożenie światowego bezpieczeństwa*, Journal of Modern Science nr 44(1), 2020, s. 209-226. https://doi.org/10.13166/jms/125602.
9. Hałas B., *Promocja terroryzmu w Internecie i przeciwdziałanie ze strony Unii Europejskiej*, Przegląd Geopolityczny, 40, 2022, s. 121-133.
10. Kacperska E., *Terroryzm międzynarodowy jako problem globalny współczesnej gospodarki*, Zeszyty Naukowe Szkoły Głównej Gospodarstwa Wiejskiego. Ekonomika i Organizacja Gospodarki Żywnościowej, nr 120, 2017, s. 17-31. https://doi.org/10.22630/EIOGZ.2017.120.36.
11. Libora G., *Oblicza współczesnego terroryzmu. Wydanie I*, Wydawnictwo internetowe e-bookowo, 2016.
12. Łuczkowska M., *Działaniu Unii Europejskiej w zakresie zwalczania terroryzmu*, Rocznik Bezpieczeństwa Międzynarodowego, vol. 10, nr 2, 2016, s. 124-133. https://doi.org/10.34862/rbm.2016.2.13.
13. Sobowiec K., *Terroryzm jako jedno z największych zagrożeń bezpieczeństwa współczesnego świata,* [w:] *Budowanie poczucia bezpieczeństwa w czasach pandemii oraz zagrożenia terroryzmem i wojną*, red. E. Jasiuk, A. Chochowska, Oficyna Wydawnicza Uczelni Łazarskiego, Warszawa 2023, s. 186.
14. Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Zeszyty Naukowe Akademii Marynarki Wojennej, Rok XLVI, nr 1(160), 2005, s. 173-181.
15. Terroryzm w UE: ataki, ofiary śmiertelne i zatrzymania w 2023 r., Parlament Europejski, https://www.europarl.europa.eu/topics/pl/article/20250124STO26468/terroryzm-w-ue-ataki-ofiary-smiertelne-i-zatrzymania-w-2023-r.
16. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2002 Nr 74, poz. 676).
17. Wardin K., *Al-Kaida Internacjonalizacja terroryzmu samobójczego*, Rocznik Bezpieczeństwa Międzynarodowego, nr 2, 2019, s. 177-189.
18. Żurawski S., Oskierko M., *Actions of the Border Guard in the event of a terrorist attack at the airport*, Studia Bezpieczeństwa Narodowego, nr 32, 2024, s. 63-80. https://doi.org/10.37055/sbn/186196.

dr Dariusz Brążkiewicz
Akademia Bialska im. Jana Pawła II
ORCID 0000-0002-5372-1210

lic. Rafał Mazurek
Akademia Sztuki Wojennej w Warszawie
https://doi.org/10.29316/9788368103199_5

WSPÓŁCZESNE POWIETRZNE DRONY ROZPOZNAWCZO-BOJOWE I ICH UŻYCIE ORAZ ZWALCZANIE NA PRZYKŁADZIE WOJNY ROSYJSKO-UKRAIŃSKIEJ

MODERN AIR RECONNAISSANCE AND COMBAT DRONES. THEIR USE AND COMBATING THEM ON THE EXAMPLE OF THE RUSSIAN-UKRAINIAN WAR

Streszczenie

Toczący się konflikt zbrojny rosyjsko-ukraiński od 2022 roku pokazuje bardzo duże zmiany w sposobie prowadzenia walki. Zmiany te dotyczą dość dużego użycia bezzałogowych statków powietrznych wspierających rozpoznanie oraz bezpośrednie atakowanie celów przeciwnika. Te nowe narzędzia walki spowodowały przewartościowania na współczesnym polu walki, wskazując na duże znaczenie tego rodzaju uzbrojenia. Uzbrojenia, wielokrotnie wykonywanego przez samych żołnierzy z połączenia dronów cywilnych i amunicji wojskowej. Przedmiotem badań niniejszej pracy jest znaczenie bezzałogowych

Summary

The ongoing Russian-Ukrainian armed conflict since 2022 has shown very significant changes in the way combat is conducted. These changes involve the relatively large use of unmanned aerial vehicles supporting reconnaissance and direct attacks on enemy targets. These new combat tools have led to reevaluations on the modern battlefield, indicating the great importance of this type of weaponry. Armament, often made by soldiers themselves from a combination of civilian drones and military ammunition. The subject of the research of this work is the importance of unmanned aerial vehicles (drones) and

statków powietrznych (dronów) i środków ich zwalczania we współczesnych konfliktach zbrojnych. Celem pracy jest przedstawienie bezzałogowych statków powietrznych i ich wykorzystanie na wojnie rosyjsko-ukraińskiej. W związku z przedmiotem badań i celem badań, powstał główny problem badawczy, który został wyrażony w postaci następującego pytania: Jakie znaczenie mają bezzałogowe statki powietrzne na współczesnym polu walki i jakie są ich możliwości w prowadzonych działaniach wojskowych? Poszukiwanie naukowych rozstrzygnięć, w odniesieniu do określonego głównego problemu badawczego, wymagało przyjęcia i rozwiązania szczegółowych problemów badawczych: 1) Jaki jest podział bezzałogowych statków powietrznych i możliwości ich bojowego użycia? 2) Jaka jest skala wykorzystania systemów zwalczających bezzałogowe statki powietrzne? 3) Jak realizowane było dotychczasowe wykorzystanie bezzałogowych statków powietrznych na przykładzie wojny rosyjsko-ukraińskiej? Przeprowadzone badania wstępne, określony cel badań i problemy badawcze zdeterminowały przyjętą na potrzeby badań hipotezę główną: Współczesne pole walki ulega kolejnym przeobrażeniom pod wpływem nowych środków walki, którymi są coraz nowocześniejsze bezzałogowe statki powietrzne. Weryfikacji dostępnych materiałów dokonano poprzez analizę i krytykę dostępnej literatury przedmiotu oraz faktów z informacji prasowych.

Słowa kluczowe: bezzałogowe statki powietrzne, drony, wojna rosyjsko-ukraińska

means of combating them in modern armed conflicts. The aim of the work is to present unmanned aerial vehicles and their use in the Russian-Ukrainian war. In connection with the subject of the research and the purpose of the research, the main research problem arose, which was expressed in the form of the following question: What is the importance of unmanned aerial vehicles on the modern battlefield and what are their capabilities in military operations? The search for scientific solutions, in relation to the specified main research problem, required the adoption and solution of detailed research problems: 1) What is the division of unmanned aerial vehicles and their combat use capabilities? 2) What is the scale of use of systems combating unmanned aerial vehicles? 3) How has the use of unmanned aerial vehicles been implemented so far, using the example of the Russian-Ukrainian war? The preliminary research conducted, the specified research goal and research problems determined the main hypothesis adopted for the research: The modern battlefield is undergoing further transformations under the influence of new means of combat, which are increasingly modern unmanned aerial vehicles. The verification of available materials was carried out by analyzing and criticizing the available literature on the subject and facts from press releases.

Keywords: unmanned aerial vehicles, drones, Russian-Ukrainian war

Wstęp

Współczesny postęp technologiczny w cyfryzacji i miniaturyzacji spowodował dość gwałtowny rozwój bezzałogowych statków powietrznych (BSP), zwanych w skrócie dronami. Motorem ich rozwoju były przede wszystkim prace prowadzone na rzecz wojska. Prace te, w pierwszej kolejności, doprowadziły do opracowania kilkadziesiąt lat temu dużych BSP, wielkości samolotów

pilotowanych przez człowieka. W ostatnich kilkunastu latach kolejne technologie i unowocześnienia spowodowały rozwój mniejszych BSP, mniej widocznych, służących do rozpoznania oraz do jednorazowego użycia, jako latające pociski.

Przez kilkanaście lat rozwijano tę broń, nie przewidując do końca jej możliwości użycia w faktycznych konflikcie zbrojnym i to na masową skalę. Nie rozwijano też systemowych sposobów przeciwdziałania im oraz zwalczania. Dopiero wybuch wojny rosyjsko-ukraińskiej w 2022 r. rozpoczął erę powietrznych dronów rozpoznawczych i uderzeniowych. Skala użycia tej technologii unaoczniła walczącym stronom oraz obserwatorom zagranicznym, jaką przewagę mają te środki walki wobec żołnierzy, a szczególnie wobec uzbrojenia i sprzętu. Duży procent zniszczeń na polu walki jest zasługą dronów powietrznych, które nie mają sobie równych w środowisku lądowym czy morskim, mimo dużych postępów strony ukraińskiej w użyciu dronów morskich. Sytuacja ta doprowadził również do intensywnego rozbudowywania systemów zwalczania fizycznego i elektronicznego tych środków walki.

Charakterystyka powietrznych dronów rozpoznawczo-bojowych we współczesnych siłach zbrojnych

Statki powietrzne były marzeniem wielu badaczy, naukowców czy artystów począwszy od samego Leonardo da Vinci. Przez ten długi okres (od XV do XXI wieku) nastąpiło wiele zmian w ich postrzeganiu. Przede wszystkim zmianie uległa wielkość – przez wiele lat samoloty były duże, przeznaczone do pilotowania przez człowieka, a obecnie najmniejsze, bezzałogowe statki powietrzne są wielkości monety. Początkowo BSP, ze względu na koszty, były wykorzystywane do celów militarnych, obecnie istnieje szeroki wybór bezpilotowych statków cywilnych, których obsługą może zająć się nawet dziecko[1].

Pierwszy raz określenie „dron" (ang. drone, pol. truteń) użyto w 1936 roku w sposób żartobliwy do przerobionej na zdalnie sterowaną konstrukcję samolotu Gavilland Tiger Moth, którego drugą nazwą była Queen Bee[2].

[1] R. Kopeć, O. Wasiuta, T. Wójtowicz, *Wojna dronów. Militarne wykorzystanie bezzałogowych statków powietrznych*, Wydawnictwo Naukowe UP, Kraków 2021, s. 30.

[2] *Zastosowanie dronów oraz ich historia*, [dostęp: 02.06.2017], portal megadron.pl, https://megadron.pl/pl/blog/zastosowanie-dronow-oraz-ich-historia-1536843674.html?srsltid=AfmBOoqm6BS8tvNad-qcLSLDuKZ-R8nmZEhma_RwBL4uGyqvkMTk9CHC, [dostęp: 10.01.2024].

Biorąc pod uwagę różnice konstrukcyjne, wyróżnia się pięć rodzajów i klas BSP, z których najczęściej używane do zadań bojowych znajdują się na trzech pierwszych miejscach poniższej listy:

- Wielowirnikowce- „koperty",
- ze stałym skrzydłem- „szybowce",
- BSP typu kombinowanego- „tiltrotory",
- sterowce i balony,
- wiatrakowce.

Klasyfikacja wagowa BSP przedstawia się następująco:

- powyżej 2000 kg – bardzo ciężkie,
- od 200 do 2000 kg – ciężkie,
- od 50 do 200 kg – średnie,
- od 5 do 50 kg – lekkie,
- do 5 kg – mikro[3].

Ze względu na długość i zasięg lotu podział jest następujący:

- powyżej 24 godzin i ponad 1500 km – wysoki,
- od 4 do 24 godzin i od 100 do 400 km – średni,
- maksymalnie 5 godzin i do 100 km – niski[4].

Wśród małych dronów największą popularnością cieszą się drony z technologią First Person View (FPV), które pozwalają na pilotowanie pojazdem sterowanym radiowo z punktu widzenia pilota za pomocą kamery na tym pojeździe. Do sterowania FPV służą gogle lub obraz monitora.

W związku z tym, że drony FPV są jednymi z mniejszych, dzielone są ze względu na gabaryty jednostki i rozstaw:

- 55-75 mm – Tinywhoop,
- ok. 2 cali – Toothpick,
- 2-3 cale – Cinewhoop,
- 4-5 cali – Freestyle,
- pow. 5 cali – Cinelifter[5].

[3] K. Balcer, *Klasyfikacja bezzałogowych statków powietrznych w odniesieniu do specyfikacji oraz przepisów prawa polskiego i międzynarodowego*, Developments in Mechanical Engineering, nr 17(9), Wydawnictwa Uczelniane Politechniki Bydgoskiej im. Jana i Jędrzeja Śniadeckich, Bydgoszcz 2021, s. 6.

[4] Ibidem, s. 7.

[5] *Rodzaje dronów FPV*, 26.07.2022, portal wgoglach.pl, https://wgoglach.pl/rodzaje-dronow-fpv/, [dostęp: 01.03.2025].

Należy również wspomnieć, że do obsługi dronów wymagane jest kilka składowych, w tym system kontroli, system telekomunikacyjny, wyposażenie odpowiednie do celów realizowanego zadania[6].

Obecne wykorzystanie dronów na płaszczyźnie militarnej obejmuje trzy kategorie działań: rozpoznawcze, bojowe i logistyczne. Należy jednak zauważyć, że pierwszym wykorzystaniem, dla którego tworzono drony było rozpoznanie, na podobieństwo wykorzystywanych od lat satelitów.

Działania rozpoznawcze z wykorzystaniem BSP pozwalają na samodzielne zbieranie informacji na wymagającym polu walki (przeszkody terenowe naturalne lub stworzone przez człowieka) poprzez dowódców kompanii czy plutonu. Wyróżnia się dwa sposoby prowadzenia obserwacji: „wiszenie i wpatrywanie się" (ang. hover and stare) polega na wyprowadzeniu statku powietrznego w określone miejsce nad powierzchnią ziemi i obserwację terenu, oraz „siedzenie i wpatrywanie się" (ang. perch and stare) polegające na wylądowaniu dronem w dogodnym miejscu pozwalającym na obserwację przy minimalnym zużyciu akumulatorów[7].

Obiekty zainteresowania wojskowych zwiadowczych BSP można podzielić na dwie kategorie:

- cele wojskowe – kosztowny lub ważny sprzęt wojskowy (radary, OPL), sprzęt ciężki (czołgi, artyleria), śmigłowce i samoloty, magazyny amunicji, obiekty logistyczne, punkty koncentracji personelu, kwatery główne personelu wojskowego, punkty kontrolne, poligony,
- cele cywilne – cywilny sprzęt ciężki mogący służyć do budowy umocnień (koparki, dźwigi, wywrotki), magazyny żywności, linie i węzły kolejowe, mosty i przeprawy, magazyny paliwa, elektrownie, obiekty przemysłowe produkujące sprzęt militarny[8].

[6] M. Terebecki, *Wykorzystanie nowoczesnych technologii przez wojska obrony terytorialnej podczas działań - roje dronów*, Zeszyty Naukowe Pro Publico Bono, nr 1, Akademia Pożarnicza, Warszawa 2022, s. 17.

[7] D. Becmer, *Bezzałogowe systemy latające klasy I - II w przyszłym systemie walki*. Zeszyty Naukowe WSOWL, nr 1(143), Wrocław 2007, s. 39-43.

[8] С. Бескрестнов, *Інструкція з протидії активності розвідувальних БПЛА РФ у прифронтовій зоні*, Київ 2024, s. 2.

Działania transportowe odbywające się za pomocą bezzałogowych statków powietrznych stanowią idealne rozwiązanie w przypadku, kiedy potrzebne jest zaopatrzenie na trudno dostępnym terenie, w którym operują siły[9].

Działania bojowe – ataki dronów można podzielić na kilka kategorii, w zależności od sposobu operowania: klasyczny – identyfikacja celu przez drona rozpoznawczego i użycie drona FPV do neutralizacji; darmowe polowanie – wykrycie i atak odbywa się jedynie dronem FPV; FPV-roy – uderzenie grupowe dronów kamikaze na wcześniej wykryty przez zwiadowczy BSP cel; towarzyszenie atakowi drużyny szturmowej za pomocą dronów FPV; dron FPV w zasadzce – lądowanie dronem FPV w niewidocznym miejscu i wyczekiwanie przeciwnika; uderzenie kombinowane – dron FPV kamikadze jest wykorzystywany do unieruchomienia pojazdu, a dron „bombowiec" zrzuca ładunek na załogę opuszczającą pojazd (możliwe odwrotne zastosowanie); podwójne uderzenie – wykorzystywane do zdobywania umocnień, pierwszy dron FPV służy do uszkodzenia lub zniszczenia bariery, drugi z ładunkiem termo barycznym lub odłamkowym do neutralizacji celu; pułapka FPV (warianty) – montowanie nadajnika GPS w konstrukcji w celu śledzenia personelu, który znalazł i zabrał obcy dron / implementowanie niewielkich ilości (20-50g) ładunku wybuchowego w konstrukcji, który w procesie demontażu zostaje aktywowany itp.; FPV Miner – przenoszenie oraz instalowanie min przeciwpiechotnych i przeciwczołgowych przez drona; Saper FPV – zrzucanie ładunków wybuchowych na wykryte wcześniej miny w celu wywołania wtórnej detonacji; Reset FPV – zrzut amunicji dronem FPV na wykryty cel przez zwiadowcę-BSP (często eliminowanie pojedynczych/grup żołnierzy); Smok FPV – rozpylanie mieszanek zapalających (między innymi termit) nad terenem wroga; FPV-PVO – zniszczenie wrogiego drona-zwiadowcy poprzez wlecenie w niego dronem FPV i staranowanie lub detonację ładunku odłamkowego podczas podejścia do taranowania; Sabotażysta FPV – wcześniejsze zaprogramowanie grupy dronów (najczęściej 4-6 sztuk) na atak kamikadze na konkretne współrzędne, pozostawione drony zostają po czasie „wybudzone" za pomocą sygnału GSM i przeprowadzają atak; FPV na macicy – wykorzystanie większego drona-matki do transportu 2-3 pomniejszych dronów FPV kamikadze. Dron matka służy również jak zwiększenie zasięgu ataku (dodatkowa antena) poprzez jego zwielokrotnienie; FPV-on-wires – prowadzenie

[9] P. Polkowski, *Bezzałogowe statki powietrzne*, Rocznik Bezpieczeństwa Międzynarodowego, tom 10, nr 1, Wydawnictwo Naukowe DSW, Wrocław 2016, s. 241.

ataków dronami sterowanymi za pomocą światłowodu (metoda niemożliwa do zakłócenia, gdyż odbywa się „po kablu"); Inspekcja budowlana – wykorzystywanie dronów mikrokopterów do rozpoznania wnętrza budynków; FPV muzzleloader – wykorzystywanie drona FPV z podwieszonym głośnikiem, który wykorzystywany jest do emisji sygnałów dźwiękowych (np. „jesteście otoczeni, w przypadku poddania gwarantowane przeżycie") służących do walki psychologicznej; Swiping – wykorzystywanie drona FPV do zrzutu ulotek informacyjnych na pozycje wroga[10].

Powyższy opis metod atakowania pozycji przeciwnika, neutralizacji siły żywej i jego zdolności bojowej ukazuje najpopularniejsze zastosowanie dronów komercyjnych z podwieszonymi ładunkami (jednymi z częściej spotykanych na wojnie rosyjsko-ukraińskiej są konstrukcie dronów-kamikadze z podwieszonym granatem RPG-7)[11].

Rozwój technologiczny oraz zmiany w strategiach prowadzenia wojen doprowadziły do wykorzystywania informacji o szczególnym znaczeniu, w tym rozpoznania satelitarnego, wywiadowczego czy systemów walki radioelektronicznej. Wojna w Ukrainie rozpoczęta przez Rosję 24 lutego 2022 roku ukazała, że nasycenie pola walki czujnikami i efektorami niezależnie od warunków pogodowych, pory roku, dna i nocy, nie daje stuprocentowej zdolności kamuflażu i przeciwdziałania BSP[12].

Systemy walki radioelektronicznej i bojowej w zwalczaniu powietrznych dronów

Wojna informacyjna poprzez rozwój technologiczny przeszła również na płaszczyznę cyfrową. W związku z potrzebą poszerzania możliwości aparatu ochrony, przejęcia lub zniszczenia informacji, przyjęto pojęcie walki radioelektronicznej (WRE). WRE obejmuje działania na poziomie militarnym

[10] *DIRECTORY. Tactics of use by the enemy FPV drones (in diagrams) and ways to counteract it*, November 9, 2024, Portal Defcad, https://defcad.com/library/tactics-of-using-fpv-drones-by-the-enemy-in-diagrams-and-methods-of-counteraction-eng/, [dostęp: 21.01.2025].

[11] P. Laskowski, *Broń precyzyjna a czołgi - zagrożenia dla pojazdów pancernych na współczesnym polu walki*, Przegląd Geopolityczny, t. 49, Polskie Towarzystwo Geopolityczne, Warszawa 2024, s. 109.

[12] R. Białoskórski, *The Theoretical Concept of Information Warfare: A General Outline*, Humanities and Social Sciences, t. 30, nr 4, Politechnika Rzeszowska, Rzeszów 2023, s. 12-13.

wykorzystujące energię elektromagnetyczną, nakierowaną na uzyskanie kontroli nad widmem elektromagnetycznym wroga (obejmuje również atak)[13].

Wojna elektroniczna, w swojej złożoności posiada systemy elektrooptyczne służące do komunikacji, prowadzenia działań ofensywnych oraz defensywnych, jakimi niewątpliwie są przeciwdziałanie penetracji własnych zabezpieczeń oraz pozycji za pomocą bezzałogowych statków powietrznych. Elektrooptyka to połączenie elektroniki i optyki, definiowana również jako nauka i technologia generowania, modulacji, wykrywania i pomiaru lub emitowania promieniowania optycznego z wykorzystaniem środków elektrycznych. Można wyróżnić wiele elektrooptycznych systemów walki elektronicznej, które działają w części widma elektromagnetycznego. Do wyżej wymienionych systemów zaliczane są między innymi czujniki podczerwieni oraz lasery, które posiadają szerokie zastosowanie, od naprowadzania systemów celowniczych oraz uzbrajania głowic bojowych poprzez pełnienie innych celów ofensywnych[14].

Ze zjawiskiem impulsu elektromagnetycznego zetknięto się przy pierwszych amerykańskich testach nad bronią jądrową, lecz do czasu drugiej wojny światowej nie przykładano do tego zjawiska zbyt dużej uwagi[15].

W walce elektronicznej można wyróżnić trzy zasadnicze płaszczyzny działania:

- rozpoznanie radioelektroniczne – to poddawanie ciągłej analizie emisji fal elektromagnetycznych, mające na celu zidentyfikowanie oraz zlokalizowanie źródła zagrożenia,
- ochrona radioelektroniczna – to zabezpieczenie wszelakich systemów, infrastruktury oraz pojazdów wojskowych, jak i personelu przed skutkami ataków obcych środków walki radioelektronicznej,

[13] K. Karcz, A. Sitkiewicz, J. Błaszczyk, Z. Mierczyk, *New Electromagnetic Threat Protection Systems*, Problemy Mechatroniki: uzbrojenie, lotnictwo, inżynieria bezpieczeństwa t. 14, nr 4, Wojskowa Akademia Techniczna, Warszawa 2023, s. 60-62.

[14] *Electronic warfare and radar systems engineering handbook (4th ed.)*, Naval Air Warfare Center, California 2013, s. 312.

[15] A. Sitkiewicz, K. Karcz, *Zagrożenia bezpieczeństwa systemów teleinformatycznych w obszarze infrastruktury krytycznej w przestrzeni kosmicznej*, [w:] *Polacy o Kosmosie. Sektor kosmiczny w perspektywie prawa, polityki i bezpieczeństwa*, red. nauk. M. Jabłoński, M. Ulański, Z. Popowicz, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń 2024, s. 140

- atak radioelektroniczny – ma na celu zmniejszenie zdolności bojowych poprzez wykorzystanie energii elektromagnetycznej do niszczenia lub zakłócania systemów, infrastruktury czy personelu przeciwnika[16].

Obecność innowacji w działaniach wojennych zawsze wiąże się z powstaniem środków przeciwdziałających, w przypadku dronów powietrznych ta zasada również znajduje swoje potwierdzenie. Zasadniczą kwestią pozostaje wyważenie relacji kosztów względem efektów przeciwdziałania, gdyż używanie bardzo kosztownego sprzętu (etatowych środków bojowych, np. rakiety przeciwlotnicze) do neutralizacji komercyjnego urządzenia wartego w okolicach 150-200 euro, jest skrajnie niewspółmierne.
Walkę z bojowymi dronami powietrznymi można podzielić na dwie płaszczyzny:

- kinetyczną – fizyczna eliminacja,
- niekinetyczną – systemy przeciwdronowe[17].

Klasyczne systemy przeciwlotnicze są ważnym elementem w walce z bezzałogowcami, lecz ze względu na relację koszt-efekt oraz po wzięciu pod uwagę, że zużycie zapasów rakiet przeciwlotniczych uszczupla możliwości przechwytujące systemu obrony powietrznej, pożądane są lepiej wyważone rozwiązania. Firma Raytheon produkuje kompletne systemy przeciwdronowe Counter-Unmanned Aerial System (C-UAS), które są jednymi z tych lepiej wyważonych pod względem efekt-koszt. W skład kompletu C-UAS o nazwie LIDS (Low, slow, small, unmanned aircraft Integrated Defeat System) spod szyldu Raytheon wchodzi: radar KuRFS (radar 360 stopni, krótkiego zasięgu, działający na paśmie Ku, które umożliwia obrazowanie w wysokiej rozdzielczości) i efektor Coyote (Coyote Block 2 jest odrzutowym efektorem kinetycznym, który skutecznie zwalcza systemy powietrzne od klasy mini do mikro UAV). Konstrukcja może występować w formie stacjonarnej lub mobilnej. System ten pozwala zwalczać bezzałogowe statki powietrzne operujące w powietrzu. Trzy elementy systemu są zintegrowane z systemem dowodzenia Forward Area Air Defense Command and Control System oraz systemami walki elektronicznej[18].

[16] K. Karcz, A. Sitkiewicz, J. Błaszczyk, Z. Mierczyk, *New Electromagnetic Threat…* op. cit.
[17] M. Mitkow, *Systemy antydronowe - konieczność na dzisiejszym polu walki [ANALIZA]*, 19.09.2023, portal defence23.pl, https://defence24.pl/przemysl/systemy-antydronowe-koniecznosc-na-dzisiejszym-polu-walki-analiza, [dostęp: 28.02.2025].
[18] Ibidem.

Polskim rozwiązaniem z dziedziny walki z dronami jest Lanca Elektromagnetyczna wyprodukowana przez PGZ S.A. Wojskowe Zakłady Elektroniczne S.A. Lanca 2.0 jest systemem przenośnym – plecakowym (waga oscyluje w okolicach 7 kilogramów, razem z anteną) – emitującym zakłócenia elektromagnetyczne (od 100 MHz do 6 GHz), ich zasięg szacowany jest na 100-300 metrów przy mocy 1 W, natomiast neutralizacja celów możliwa jest na dystansie do 1000 metrów (obejmuje pasma 0,42-0,45 GHz, 2,4-2,5 GHz, 5,7-5,8 GHz)[19].

Do systemów C-UAS zaliczana jest również broń laserowa, wykorzystująca fotony do neutralizacji celów. Technologia zwana HEL (High Energy Laser) producenta Raytheon, to laser o wysokiej mocy (istnieją dwie wersji, słabsza o mocy 15kW oraz mocniejsza, o mocy 50kW), który zintegrowany z systemem na bazie pojazdu Stryker potrafi wykrywać, śledzić oraz eliminować cele pojedyncze, jak i „roje" dronów. Rozwiązanie to jest również korzystne, jeśli mówimy o bezpieczeństwie otoczenia, gdyż podczas eliminacji celów wysyłana jest jedynie cząstka światła, niepowodująca efektów kinetycznych[20].

Ze względu na niskie koszty implementacji i eksploatacji komercyjnych bezzałogowców, stosunek kosztów przeciwdziałania im do wartości urządzenia, jest drastyczny. Sytuacja zmienia się w momencie, kiedy za cel obierani są operatorzy tych urządzeń. Proces profesjonalnego wyszkolenia pilota bezzałogowca jest długotrwały i wymaga specjalistycznej wiedzy z wielu dziedzin. Wyróżnia się trzy sposoby fizycznej lokalizacji i eliminacji operatorów: kontr obserwacja BSP i naprowadzanie ognia artyleryjskiego; zbieranie danych z systemu Aeroscope; odnajdowanie metodą triangulacji sygnału wysyłanego przez kontrolera do jednostki latającej[21].

Siły Zbrojne Federacji Rosyjskiej rozwinęły niekonwencjonalny sposób walki z ukraińskimi dronami komercyjnego producenta DJI. Wykorzystują system DJI Aeroscope, umożliwiający śledzenie lokalizacji dronów (jedynie konstrukcji DJI) w czasie rzeczywistym oraz miejsca dyslokacji pilotów

[19] M. Dąbrowski, *MSPO 2019: Elektromagnetyczne Lance przeciwko dronom*, 06.09.2019, portal defence24.pl, https://defence24.pl/przemysl/mspo-2019-elektromagnetyczne-lance-przeciwko-dronom, [dostęp: 01.03.2025].

[20] Ibidem.

[21] S. Mitkow, J. Antczak, M. Roszkiewicz, *Zarządzanie innowacjami w przemyśle zbrojeniowym przy współpracy startupu jako istotny element budowy bezpieczeństwa w dobie zagrożenia ze Wschodu*, Studia Wschodnioeuropejskie, nr 19, Warszawa 2023, s. 244.

posługujących się nimi, dalszy proces eliminacji wrogich pilotów odbywa się w zależności od posiadanych sił i środków przeznaczonych do tego celu[22].

Warto również dodać, że fizyczna eliminacja wrogich dronów za pomocą broni osobistej bądź zespołowej, nadal jest jedną z częstszych metod eliminacji zagrożenia z ich strony[23]. Stosowane są również wszelkiego rodzaju siatki, mające na celu zablokowanie drona i niedopuszczenie go do celu i neutralizując tym zagrożenie. Do wystrzelenia takowej siatki używana jest ręczna wyrzutnia, istnieją również inne drony posiadające mechanizmy zrzutowe siatek antydronowych. Rozwiązanie to powoduje unieruchomienie elementów odpowiedzialnych za napęd i sterowanie bezzałogowym statkiem powietrznym. Mimo dużej zalety jaką jest niewielki koszt tego rozwiązania, na pierwszy plan wysuwa się duża wada, jaką jest niewątpliwie – krótki zasięg – co uniemożliwia w tym wypadku walkę prowadzoną z ziemi z dronami operującymi na wysokich pułapach oraz celność zależną od wielu czynników (operatora systemu antydronowego, motywacji agresora nie chcącego stracić własnego urządzenia)[24].

Walka z bezzałogowymi statkami powietrznymi przeciwnika, to nie tylko fizyczna eliminacja, to również wszelkie działania mające na celu ograniczenie możliwości wykrycia oraz naprowadzenia ognia przez wroga. W czasie walki należy wziąć pod uwagę, że wrogie BSP mogą latać nad „strefą zainteresowania", nie będąc przy tym wykrytym przez detektory, z tego powodu w miarę możliwości operacyjnych powinno się zawsze przestrzegać poniższych zasad:

- sprzęt wojskowy maskować nawet 40-50 kilometrów od linii frontu,
- jeśli zakamuflowanie pojazdu stanowi poważny problem, nie należy dopuszczać do gromadzenia się ich w pobliżu siedzib i mieszkań personelu,
- unikać gromadzenia pojazdów na terenach wydarzeń szkoleniowych i treningowych,
- w miarę możliwości unikać zatrzymywania sprzętu wojskowego na publicznych stacjach benzynowych,

[22] Ibidem.

[23] Ibidem.

[24] M. Świeczkowski, *Technologiczna odpowiedź struktur bezpieczeństwa portu na zagrożenia ze strony bezzałogowych statków powietrznych*, Rocznik bezpieczeństwa morskiego rok XIII, Akademia Marynarki Wojennej im. Bohaterów Westerplatte, Gdynia 2019, s. 237.

- unikać dłuższego (ponad 10-15minut) zatrzymywania się sprzętem wojskowym na autostradach i drogach,
- jeśli pojazd uległ awarii na drodze lub autostradzie i jest pozbawiony możliwości mobilnych, nie pozostawać w nim. Podczas przystępowania do holowania uszkodzonego pojazdu, należy bacznie obserwować niebo,
- unikać gromadzenia sprzętu budowlanego (wykorzystywanego do budowy umocnień) na otwartych przestrzeniach,
- nie dopuszczać do wzmożonego ruchu pojazdów wojskowych w okolicach punktów logistycznych. Należy rozplanować pobieranie zasobów równomiernie,
- planować wykonanie działań militarnych i logistycznych po zmroku (większość dronów pozbawiona jest kamer termowizyjnych),
- wykorzystywać trudne warunki pogodowe do przeprowadzania ważnych manewrów sprzętu i personelu,
- unikać systematycznej działalności (np. dowóz paliwa z punktu logistycznego, w każdy poniedziałek, o określonej godzinie)[25].

W przypadku otrzymania informacji o obecności wrogiego rozpoznawczego BSP nad własnymi pozycjami należy „nie zwracać" na siebie uwagi pilota, ponieważ obserwując pole, gdzie nie można zaznaczyć wzmożonej aktywności lub innych oznak działalności wojsk, obszar zostanie zaklasyfikowany jako „nieciekawy". Dlatego w takiej sytuacji powinno przestrzegać się następujących zasad:

- pojazdy poruszające się po drogach nie mogą się zatrzymywać,
- osoby nie powinny wychodzić na otwartą przestrzeń i w tym czasie przemieszczać się,
- należy wykluczyć poruszanie się pojazdów wojskowych w obszarze obserwowanym,
- należy ukryć ciężki sprzęt wojskowy i cywilny,
- zaprzestać pracy artylerii dalekiego zasięgu rozlokowanej na obserwowanym terytorium,
- wojskowe ciężarówki nie kierują się do składów broni i magazynów,
- skupiska sprzętu znajdujące się na otwartej przestrzeni należy rozproszyć, natomiast jeśli BSP wroga jest już za blisko, lepiej zaniechać czynności rozpraszających[26].

[25] С. Бескрестнов, *Інструкція з протидії...,* op. cit., s. 3-4.

[26] Ibidem, s. 4-5.

Drony rozpoznawczo-bojowe i systemy ich zwalczania w konflikcie rosyjsko-ukraińskim

Na przestrzeni trzech lat wojny powietrzne drony bardzo mocno wpisały się we współczesne działania wojskowe. Głównie obejmują one działania w bezpośrednim kontakcie bojowym na pierwszej linii ognia, jak i też w głębi obrony czy ataku. Tym samym efektywny promień działania drona to ok. 5 km. Ponadto istnieją bezzałogowe statki powietrzne z głowicami bojowymi, przeznaczone do atakowania głównie obiektów, na zapleczu nieprzyjaciela. Wszystkie te możliwości są wykorzystywane na wojnie rosyjsko-ukraińskiej.

Pierwsze tygodnie wojny rosyjsko-ukraińskiej rozpoczętej przez Rosję 24 lutego 2022 roku nagłośniły znaczenie bezzałogowych statków powietrznych w związku z użyciem Bayraktarów TB2 operujących po stronie ukraińskiej[27]. Jest to turecka konstrukcja taktycznego bezzałogowego systemu rozpoznawczo-uderzeniowego (BSR-U), wykorzystywana jednocześnie do zadań związanych z kontrolą obserwacyjną i możliwością wykonania uderzenia. Ta konstrukcja ma możliwość osiągnięcia lotu długości 27 godzin, a jego maksymalna prędkość wynosi 220 kilometrów na godzinę[28]. Pierwszy atak za pomocą Bayraktara TB2 na kolumnę wojsk rosyjskich zmierzających w stronę Kijowa miał miejsce 27 lutego 2022 roku, a przez połowę marca wyżej wymieniony dron stanowił śmiertelne zagrożenie dla rosyjskich kolumn. Pod koniec marca po rozciągnięciu przez stronę rosyjską skutecznej ochrony przeciwlotniczej znaczenie uderzeniowe Bayraktarów zmalało[29].

Dla odmiany w pierwszej fazie wojny Rosjanie w sposób ograniczony wykorzystywali drony, ale w trakcie walk zaczęli je stosować głównie do eliminacji uzbrojenia i sprzętu wojskowego oraz żołnierzy w strefie walk. W drugiej połowie 2022 r. Rosjanie zaczęli używać w większej ilości dronów kamikadze o nazwie Lancet. Rosjanie zdobyli dzięki nim doświadczenie i obecnie w użyciu pojawiają się udoskonalone ich wersje. Analitycy wojskowi stwierdzają, że drony Lancet 3 to jedne z najlepszych tego typu urządzeń na świecie. Ich atutem jest układu skrzydeł wykonanych w kształcie litery X, pozwalający

[27] *Bayraktar - Ukrainian War Song (English subtitles, napisy polskie and other languages)*, 23.05.2022, portal youtube.com, https://www.youtube.com/watch?v=S3FGWPMjl6M, [dostęp: 22.01.2025].

[28] *Bezzałogowce BAYRAKTAR TB2*, portal gov.pl, https://www.gov.pl/web/obrona-narodowa/bezzalogowce-bayraktar-tb2, [dostęp: 22.01.2025].

[29] R. Rochowicz, *Drony w wojnie Ukrainy z Rosją*, Zeszyty 160 nr 2, Wojskowy Instytut Techniczny Uzbrojenia, Zielonka 2022, s. 108-109.

na niezwykle szybką zmianę kierunku lotu. Dlatego na przestrzeni trzech lat wojny potrafiły zadać dotkliwe straty Siłom Zbrojnym Ukrainy[30]. Dla przykładu jedna z pierwszych utraconych polskich armatohaubic Krab 155 mm w składzie wojsk ukraińskich została właśnie zniszczona w listopadzie 2022 r. przez tego typu drona – Lancet 3. Są one użytkowane głównie przez jednostki specnazu[31].

Mimo wcześniejszej obecności dronów powietrznych w konflikcie rosyjsko-ukraińskim powstanie na mocy dekretu odrębnych od pozostałych wojsk ukraińskich Sił Systemów Bezzałogowych SZ Ukrainy, miało miejsce 6 lutego 2024 roku. Było to działanie rozwijające znaczenie systemów dronowych operujących w powietrzu, morzu i na ziemi, tak widocznych od początku konfliktu w 2022 roku[32].

Wśród zadań, które ma spełniać nowo utworzony rodzaj wojsk ukraińskich znajdują się między innymi:

- prowadzenie działań bojowych,
- stworzenie ujednoliconego szkolenia operatorów dronów,
- prowadzenie badań odnośnie do ewolucji taktyki ich użytkowania,
- prowadzenie eksperymentów oraz testów z systemami dronowymi[33].

Poniżej przedstawiono przykłady użycia dronów w wojnie rosyjsko-ukraińskiej w drugiej połowie 2024 roku. Sierpień oraz wrzesień 2024 roku odznaczał się zwiększoną aktywnością ukraińskich ataków systemami bezzałogowymi o średnim i wysokim zasięgu na obiekty znajdujące się na terenie Federacji Rosyjskiej. Skupiano się na atakowaniu rosyjskich baz lotniczych oraz składów amunicji. Nocą z 21 na 22 sierpnia 2024 roku przeprowadzono atak na głębokości 270 km wewnątrz Rosji. Wykorzystano drony powietrzne wyposażone w głowice odłamkowo-burzące, które spowodowały cztery główne ogniska pożarów i doprowadziły do wybuchów wtórnych, niszcząc

[30] F. Mielczarek, *Fenomen rosyjskich superdronów Lancet. Zaskakują Ukraińców*, 30 sierpnia 2023 r., portal geekweek.interia.pl, https://geekweek.interia.pl/militaria/news-fenomen-rosyjskich-superdronow-lancet-zaskakuja-ukraincow,nId,6995209, [dostęp: 16.01.2025].

[31] P. Juraszek, *Pierwszy AHS Krab zniszczony w walce. Dokonał tego rosyjski Specnaz*, 28 listopada 2022 r., portal wp.pl, https://tech.wp.pl/pierwszy-ahs-krab-zniszczony-w-walce-kulisy-brutalnej-wojny-artyleryjskiej,6838782676957888a, [dostęp: 10.02.2025].

[32] M. Gawęda, *Siły Systemów Bezzałogowych SZU. Jak Ukraina utworzyła wojska dronowe? [ANALIZA]*, 23.11.2024, portal defence24.pl, https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/sily-systemow-bezzalogowych-szu-jak-ukraina-utworzyla-wojska-dronowe-analiza, [dostęp: 10.02.2025].

[33] Ibidem.

skład amunicji oraz kilka hangarów przeznaczonych do przechowywania samolotów bojowych (Su-34 - jeden zniszczono, a drugi, prawdopodobnie uszkodzono). Trzy dni później, 25 sierpnia 2024 r. przeprowadzono atak na głębokości 700 km w głębi Rosji atakując bazę Engels, w której stacjonowały rosyjskie bombowce strategiczne Tu-95MS. 1 września 2024 r. zaatakowano zmasowanym atakiem rosyjską infrastrukturę energetyczną w obwodzie moskiewskim i twerskim, powodując uszkodzenie konakowskiej hali turbin. Osiem dni później, z 9 na 10 sierpnia 2024 roku zaatakowano rosyjskie porty lotnicze w Domodiedowie, Szeremietiewie, Żukowsku i Wnukowie, które zostały czasowo wykluczone z użytku. 18 sierpnia 2024 roku atakiem na bazę paliwową Kawkaz w obwodzie rostowskim doprowadzono do zniszczenia lub uszkodzenia 70-80% zbiorników paliwowych (łącznie na terenie bazy znajdowało się 80 zbiorników), których pożar był bardzo trudny do ugaszenia[34].

Głównymi dronami kamikadze dalekiego zasięgu wykorzystywanymi przez SZ Ukrainy są takie maszyny jak: Bóbr, Liutyj, UJ-25, Scyt oraz Piekło – dron rakieta. Odnotowano również udział drona E-300 (ma możliwość powrotu do bazy), którego udźwig pozwala na transport 250 kilogramowych bomb[35]. System Bóbr (VG-26 Bóbr) najprawdopodobniej produkowany przez ukraińską firmę UkrJet, posiada zasięg w okolicach 1000 kilometrów (w zależności od źródeł informacji, waha się od 700 do 1200 kilometrów), a maksymalny udźwig głowicy bojowej wynosi 75 kilogramów. Został użyty do ataku celów w okolicach Moskwy już w maju i lipcu 2023 roku[36]. Jego bryła została zaprojektowana w układzie „kaczki", co czyni go bardzo zwinnym bezzałogowym statkiem powietrznym (kontrola pochylenia drona w górę i w dół, nie powoduje utraty siły nośnej[37]). Poza posiadaniem wysokiej odporności na rosyjskie systemy walki radioelektronicznej jego zwinność pozwala na manewrowe uniknięcie obrony przeciwlotniczej wroga. Posiada rozpiętość

[34] M. Gawęda, *Wojna rosyjsko-ukraińska cz. 28*, Wojsko i Technika, nr 10, ZBIAM, Warszawa 2024, s. 58-59.

[35] *Wojna w Ukrainie. Zaskakujące ukraińskie naloty na Rosję*, 02.02.2025, portal rp.pl, https://www.rp.pl/konflikty-zbrojne/art41756631-wojna-w-ukrainie-zaskakujace-ukrainskie-naloty-na-rosje, [dostęp: 11.02.2025].

[36] *Bóbr dalekiego zasięgu, czyli czym Ukraińcy bombardują Rosję*, 22.01.2024, portal rp.pl, https://www.rp.pl/konflikty-zbrojne/art39728931-bobr-dalekiego-zasiegu-czyli-czym-ukraincy-bombarduja-rosje, [dostęp: 11.02.2024].

[37] *Wolontariusz Serhij Prytula pokazał drony kamikadze Bóbr*, 30.07.2023, portal mil.un.ua, https://mil.in.ua/pl/news/wolontariusz-serhij-prytula-pokazal-drony-kamikadze-bobr/, [dostęp: 11.02.2025].

skrzydeł wynoszącą 3,5 metra przy długości 2,5 metra, osiągając prędkość w okolicach 150-200 kilometrów na godzinę, pozostając w działaniu do nawet 7 godzin. Średnia wartość jednego drona Bóbr wynosi 100 tysięcy dolarów[38].

Ukraiński system dronowy dalekiego zasięgu Liutyj wykorzystywany jest do ataku na kluczowe cele położone na terytorium Federacji Rosyjskiej. Z uwagi na wysokie koszty produkcji (około 200 tysięcy dolarów za sztukę) jego użycie jest dozowane. Dron ma rozpiętość skrzydeł około 6,7 metra i długość 4,4 metra, przy wadze około 250-300 kilogramów. Konstrukcja napędzana jest silnikiem o mocy 50 koni mechanicznych, mogącym udźwignąć ładunek bojowy o wadze sięgającej 50 kilogramów. Do konstrukcji użyto włókno szklane oraz żywicę epoksydową, co przełożyło się na lepszy zasięg i udźwig w porównaniu do jego poprzednika „Bobra"[39].

Pierwsze użycie autorskiego ukraińskiego drona dalekiego zasięgu Paljanyca miało miejsce w drugiej połowie 2024 roku[40]. Jego przeznaczenie skupia się na niszczeniu lotnisk wojskowych Federacji Rosyjskiej oraz eliminacji „potencjału ofensywnego wroga". Zasięg konstrukcji napędzanej silnikiem odrzutowym oscyluje w okolicach 600-750 kilometrów[41]. Wystrzelenie pocisku-drona ma miejsce z platformy lądowej, a konstrukcyjne połączenie pocisku manewrującego z bezzałogowym statkiem powietrznym pozwala na wykonywanie precyzyjnych manewrów przy znacznie większej prędkości przelotowej (porównując do klasycznych dronów BSP lub FPV)[42].

2024 rok przyniósł przełom w walkach na terenach gęsto porośniętych roślinnością, które wcześniej były dogodnym miejscem ukrywania

[38] F. Mielczarek, *Ukraiński wywiad w końcu ujawnił swoją tajną broń*, 17.11.2023, portal geekweek.interia.pl, https://geekweek.interia.pl/lotnictwo/news-ukrainski-wywiad-w-koncu-ujawnil-swoja-tajna-bron,nId,7155614, [dostęp: 11.02.2024].

[39] S. Tetera, *Lutyj - ukraiński dron strategiczny*, 18.05.2024, portal onet.pl, https://www.onet.pl/informacje/nowa-technika-wojskowa/lutyj-ukrainski-dron-strategiczny/z50psmf,30bc1058, [dostęp: 11.02.2025].

[40] *„Znacznie szybszy i potężniejszy". Ukraina po raz pierwszy użyła nowego drona Palianyca*, 25.08.2024, portal rp.pl, https://www.rp.pl/swiat/art41017351-znacznie-szybszy-i-potezniejszy-ukraina-po-raz-pierwszy-uzyla-nowego-drona-palianyca, [dostęp: 11.02.2025].

[41] M. Górski, *Zełenski: Ukraina stworzyła nowego drona. Do czego służy Palanycia?*, 25.08.2024, portal defence24.pl, https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/zelenski-ukraina-stworzyla-nowego-drona-do-czego-sluzy-palanycia, [dostęp: 11.02.2025].

[42] R. Muczyński, *Palanycia – pocisk-bezzałogowiec w Siłach Zbrojnych Ukrainy*, 26.08.2024, portal milmag.pl, https://milmag.pl/palanycia-pocisk-bezzalogowiec-w-silach-zbrojnych-ukrainy, [dostęp: 11.02.2025].

posterunków i wyczekiwania na ruch przeciwnika. Po stronie ukraińskiej opracowano metodę wykorzystującą drony FPV wyposażone w ładunki termitu przeznaczone do zrzucenia, które w styczności z podłożem wytwarzają bardzo wysokie temperatury prowadzące do zapłonu okolicznej roślinności. Termit w Ukrainie był wykorzystywany przed 2024 rokiem do unieruchamiania rosyjskich czołgów i pojazdów. Możliwość wykluczenia znacznego obszaru za pomocą termitu, w porównaniu do dronów kamikaze atakujących punktowo, działa również na morale przeciwnika, skutecznie je obniżając. Strona rosyjska również wykorzystywała amunicję zawierającą termit, między innymi do ostrzału artyleryjskiego Mariupola, w 2022 roku. Wykorzystanie dronów FPV w połączeniu z termitem, pozwala neutralizować cele znacznie tańszym sposobem niż przy użyciu etatowych środków bojowych[43].

Natomiast 24 stycznia 2025 roku Ministerstwo Obrony Federacji Rosyjskiej opublikowało informację o zestrzeleniu dotychczas rekordowej liczby dronów. Od czwartku do piątku (23-24 stycznia 2025 roku) siły rosyjskie zniszczyły 218 dronów, z czego 174 znajdujących się poza „strefą specjalnej operacji wojskowej", czyli na terytorium Federacji Rosyjskiej. Ukraiński atak został przeprowadzony jednocześnie na 12 rosyjskich regionów, wliczając w to stolicę – Moskwę oraz Krym. Mimo informacji o sukcesach w strąceniu dużej ilości dronów, zrealizowano skuteczny atak na rosyjską fabrykę w obwodzie briańskim, co spowodowało wstrzymanie linii produkcyjnej. Zakład zajmował się produkcją elementów składowych systemów Pancyr (obrona powietrzna) oraz Iskander (system rakietowy)[44]. Tej samej nocy został przeprowadzony również skuteczny atak na rosyjską rafinerię oraz elektrociepłownię znajdującą się w Razaniu, eliminując obydwa obiekty z użytku i ograniczając zdolności produkcyjne gospodarki rosyjskiej[45].

Do walki z rosyjskimi BSP, SZ Ukrainy wykorzystują między innymi przeciwlotniczą artylerię lufową. Drugą młodość przechodzą niemieckie systemy przeciwlotnicze Gepard (produkowane od 1965 roku na podwoziu czołgu Leopard 1), wyposażone w armaty o kalibrze 35 milimetrów. Gepardy

[43] J. M. Brzezina, *Nowa broń Ukrainy. Palący się termit spada na Rosjan z dronów*, Nowa Technika Wojskowa nr 11, Warszawa 2024, s. 36-39.

[44] *Ukraina przeprowadziła największy od początku wojny atak dronów na Rosję*, 24.01.2025, portal wiadomosci.onet.pl, https://wiadomosci.onet.pl/najwiekszy-taki-atak-ukrainy-od-poczatku-wojny-174-drony/fvfx3fy, [dostęp: 25.01.2025].

[45] *„Nie ma już zakładu w Riazaniu". Pożar i zniszczenia po ataku dronów*, 24.01.2025, portal money.pl, https://www.money.pl/gospodarka/nie-ma-juz-zakladu-w-riazaniu-pozar-i-zniszczenia-po-ataku-dronow-7117604861647648a.html, [dostęp: 25.01.2025].

stanowią skuteczne narzędzie z niezbyt szybkimi dronami wykorzystywanymi przez Siły Zbrojne Federacji Rosyjskiej[46].

Skutecznym narzędziem do walki z dronami FPV jest zagłuszanie fal radiowych, na których opiera się sterowanie nimi. Do tych celów SZ Ukrainy wykorzystują między innymi nadajnik Dome EW (z racji małej dostępności – w 2024 roku firma Metinvest przekazała 100 sztuk), które montowane są na pojazdach, tymczasowych bazach i stanowiskach dowodzenia ukraińskich wojsk[47]. Urządzeniem dedykowanym do ochrony pojazdów przed atakami rosyjskich dronów i amunicji krążącej jest system z 2023 roku o nazwie Piranha-Armored Vegicle Dome 360. Posiada skuteczny zasięg 600 metrów (w okresie letnim nawet do 700 metrów), w promieniu którego BSP tracą kontakt z operatorami, awaryjnie lądują lub bezwiednie spadają nie stwarzając zagrożenia osobom przemieszczającym się w pojeździe[48].

Siły Zbrojne Federacji Rosyjskiej 26 sierpnia 2024 roku przeprowadziły pierwszy na tak dużą skalę zmasowany atak rakietowo-dronowy od początku wojny. Celem ataków była infrastruktura zaopatrująca w energię Ukrainę. Użyte przez Federację Rosyjską środki bojowe osiągnęły cel w 15 ukraińskich obwodach uszkadzając obiekt przemysłowy w obwodzie płotawskim, infrastrukturę energetyczną (zakład energetyczny w Równe) i wodną (zapora w Wyszogrodzie na rzece Dniepr) oraz rażąc 22 prywatne obiektu mieszkalne w obwodzie kijowskim[49]. Użyto w nim około 236 środków, z czego użyto 109 dronów powietrznych Shahed, resztę stanowiły pociski rakietowe trzech różnych typów. Obrona przeciwlotnicza Ukrainy zdołała zneutralizować 99 dronów i 102 rosyjskie pociski kierowane[50].

---

[46] R. Ditrich, *Sceny jak z Gwiezdnych Wojen. Tak Ukraina walczy z bezzałogowcami Geran-2*, 06.11.2024, portal forsal.pl, https://forsal.pl/swiat/ukraina/artykuly/9669711,sceny-jak-z-gwiezdnych-wojen-tak-ukraina-walczy-z-bezzalogowcami-gera.html, [dostęp: 11.02.2025].

[47] M. Tomiczek, *Systemy walki z dronami. Potrzebny sprzęt na takiej wojnie*, 06.01.2024, portal tech.wp.pl, https://tech.wp.pl/systemy-walki-z-dronami-potrzebny-sprzet-na-takiej-wojnie,6981818801076736a, [dostęp: 27.02.2025].

[48] M. Kozubel, *Nowy ukraiński system WRE przeciwko dronom przyjęty na uzbrojenie*, 11.11.2023, portal defence24.pl, https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/nowy-ukrainski-system-wre-przeciwko-dronom-przyjety-na-uzbrojenie, [dostęp: 27.02.2025].

[49] M. Strembski, *Silny atak Rosji na ukraińską infrastrukturę energetyczną*, 26.08.2024, portal portalmilitarny.pl, https://portalmilitarny.pl/wiadomosci/silny-atak-rosji-na-ukrainska-infrastrukture-energetyczna/, [dostęp: 11.02.2025].

[50] M. Gawęda, *Wojna rosyjsko-ukraińska cz. 28*, op. cit, s. 56-57.

Natomiast do największego ataku dronowego Federacji Rosyjskiej doszło dzień przed trzecią rocznicą wybuchu pełnoskalowej wojny – 21 lutego 2024 roku. Do przeprowadzenia ataku na 13 ukraińskich obwodów wykorzystano 267 dronów (większość z nich to drony Shahed). Mimo zestrzelenia przez stronę ukraińską 138 rosyjskich BSP, doszło do poważnych problemów w obwodach zaporoskim, odeskim, dniepropietrowskim, połtawskim oraz kijowskim[51].

Drony Shahed-136 (zwany również Szahid) należą do najczęściej wykorzystywanych przez Federację Rosyjską dronów irańskich w konflikcie z Ukrainą. Jest to jednostka dalekiego zasięgu mogąca operować do 1000 kilometrów (niektóre źródła podają, że zbiornik paliwa pozwala na pokonanie 2500 kilometrów), a jej udźwig wynosi do 50 kilogramów materiałów wybuchowych. Rozpiętość skrzydeł wynosi 2,5 metra, przy długości 3,5 metra, przy wadze około 200 kilogramów, napędzanych silnikiem o mocy 50 koni mechanicznych[52]. Iran dostarcza również inne modele dronów dla Federacji Rosyjskiej, a wśród nich znajdują się między innymi Shahed-131[53] i Mohajer-6[54]. Shahedy są wykorzystywane do przeprowadzania głębokich ataków na terytorium Ukrainy, a głównymi celami jest ukraińska infrastruktura krytyczna i obiekty cywilne[55]. Irańska firma IRGC Sahara Thunder sprzedała Federacji Rosyjskiej drony Shahed-136 w cenie 193 tysięcy dolarów za sztukę przy zamówieniu

[51] *Największy atak od początku agresji. Rosja wysłała ponad 250 dronów*, 2.02.2024, portal tvn24.pl, https://tvn24.pl/swiat/ukraina-najwiekszy-atak-od-poczatku-agresji-rosja-wyslala-ponad-250-dronow-st8318858, [dostęp: 27.02.2025].

[52] P. Juraszek, *Rosjanie zaatakowali Shahedami. Miały nawigację ze sprzętu rolniczego*, 03.01.2025, portal tech.wp.pl, https://tech.wp.pl/rosjanie-zaatakowali-shahedami-mialy-nawigacje-ze-sprzetu-rolniczego,7110275941415680a, [dostęp: 11.02.2025].

[53] *Rosjanie zaczęli używać dronów kamikadze Shahed-131*, 14.10.2022, portal mil.in.ua, https://mil.in.ua/pl/news/rosjanie-zaczeli-uzywac-dronow-kamikadze-shahed-131/, [dostęp: 11.02.2025].

[54] *Marynarka Wojenna Ukrainy ujawniła szczegóły o zestrzeleniu irańskiego drona nad Morzem Czarnym*, 06.06.2023, portal mil.in.ua, https://mil.in.ua/pl/news/marynarka-wojenna-ukrainy-ujawnila-szczegoly-o-zestrzeleniu-iranskiego-drona-nad-morzem-czarnym/, [dostęp: 11.02.2025].

[55] M. Mitkow, *Widziane z orbity: rosyjski magazyn dronów Shahed zniszczony*, 25.06.2024, portal space24.pl, https://space24.pl/satelity/obserwacja-ziemi/widziane-z-orbity-rosyjski-magazyn-dronow-shahed-zniszczony, [dostęp: 11.02.2025].

6 tysięcy egzemplarzy (negocjowany był zakup 2 tysięcy sztuk, w cenie 290 tysięcy dolarów za egzemplarz)[56].

Rosyjskie Wojska Radioelektroniczne, nie tak liczne w pierwszej fazie konfliktu, odznaczały się znaczącą nieporadnością w prowadzeniu ochrony własnych oddziałów i obiektów. Wyciągając wnioski z walk, przeprowadzono proces nasycenia oraz implementacji rozwiązań dostosowywanych do zwalczania ukraińskich BSP oraz dronów FPV. Plecakowe zakłócacze zostały zastosowane do zwiększenia poziomu ochrony niewielkich grup rosyjskich żołnierzy – dron po wpadnięciu w „pułapkę radioelektroniczną" wytwarzaną przez urządzenie, traci swoje możliwości[57].

Podsumowanie

Pojawienie się na współczesnym polu walki bezzałogowych statków powietrznych pokazuje, jak postęp technologii cyfrowych zmienił środowisko współczesnych konfliktów zbrojnych. Użycie dronów zmieniło oblicze wojny na Ukrainie. Tradycyjne, a jednocześnie podstawowe środki walki, takie jak czołgi, bojowe wozy piechoty czy kołowe transportery opancerzone i wyrzutnie rakietowe oraz działa artyleryjskie, muszą zostać wzmocnione o obronę przeciwko powietrznym dronom. Zagrożenie ze strony dronów już rozwinęło uzbrojenie i sprzęt do ich unieszkodliwiania i zwalczania, ale jest to proces wymagający ciągłego rozwoju tak, jak rozwijane są drony. W tym aspekcie ważna będzie zmiana uwarunkowań maskowania sprzętu i ludzi przed tym zagrożeniem. Tym samym przyszłość rozwoju i użycia powietrznych dronów przez wojsko jest jak najbardziej wskazana, co pokazują możliwości tego sprzętu, gdzie koszt pojedynczego drona jest zdecydowanie mniejszy niż niszczonych przez nie uzbrojenia i sprzętu oraz wyszkolonych żołnierzy. Ponadto ataki na obiekty infrastruktury krytycznej oraz domy mieszkalne są destrukcyjne i powodują również oddziaływanie na społeczeństwo strony przeciwnej wpływając tym samym na nastroje społeczne.

[56] M. Szopa, *Ile Rosjanie przepłacają za drony Szahid?*, 06.02.2024. portal defence24.pl, https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/ile-rosjanie-przeplacaja-za-drony-szahid, [dostęp: 11.02.2025].

[57] S. Ruszkiewicz, *Wojna dronów na froncie. „Rosjanie używają zwykłych składaków"*, 03.02.2025, portal wiadomosci.wp.pl, https://wiadomosci.wp.pl/wojna-dronow-na-froncie-rosjanie-uzywaja-zwyklych-skladakow-7121283399826240a, [dostęp: 27.02.2025].

Literatura

1. Balcer K., *Klasyfikacja bezzałogowych statków powietrznych w odniesieniu do specyfikacji oraz przepisów prawa polskiego i międzynarodowego*, Developments in Mechanical Engineering, nr 17(9), 2021, s. 5-15. DOI: 10.37660/dme.2021.17.9.1
2. Бескрестнов С., *Інструкція з протидії активності розвідувальних БПЛА РФ у прифронтовій зоні*, Київ 2024. https://nvkarta.com/project/library/uploads/military/bpla/(uk)_flash_protydiyiya_bpla_rf_u_pryfrontoviy_zoni.pdf#page=1&zoom=auto,-272,668.
3. Białoskórski R., *The Theoretical Concept of Information Warfare: A General Outline*, Humanities and Social Sciences, t. 30, nr 4, Politechnika Rzeszowska, Rzeszów 2023.
4. Becmer D., *Bezzałogowe systemy latające klasy I - II w przyszłym systemie walki*. Zeszyty Naukowe WSOWL, nr 1(143), 2007, s. 33-44.
5. Brzezina J. M., *Nowa broń Ukrainy. Palący się termit spada na Rosjan z dronów*, Nowa Technika Wojskowa nr 11, Magnum-X, Warszawa 2024.
6. *Electronic warfare and radar systems engineering handbook (4th ed.)*, Naval Air Warfare Center, California 2013.
7. Gawęda M., *Wojna rosyjsko-ukraińska cz. 28*, Wojsko i Technika, nr 10, ZBIAM, Warszawa 2024.
8. Karcz K., Sitkiewicz A., Błaszczyk J., Mierczyk Z., *New Electromagnetic Threat Protection Systems*, Problemy Mechatroniki: uzbrojenie, lotnictwo, inżynieria bezpieczeństwa t. 14, nr 4, Wojskowa Akademia Techniczna, Warszawa 2023.
9. Kopeć R., Wasiuta O., Wójtowicz T., *Wojna dronów. Militarne wykorzystanie bezzałogowych statków powietrznych*, Wydawnictwo Naukowe UP, Kraków 2021.
10. Laskowski P., *Broń precyzyjna a czołgi - zagrożenia dla pojazdów pancernych na współczesnym polu walki*, Przegląd Geopolityczny, t. 49, Polskie Towarzystwo Geopolityczne, Warszawa 2024.
11. Mitkow S., Antczak J., Roszkiewicz M., *Zarządzanie innowacjami w przemyśle zbrojeniowym przy współpracy startupu jako istotny element budowy bezpieczeństwa w dobie zagrożenia ze Wschodu*, Studia Wschodnioeuropejskie, nr 19, 2023, s. 222-249. http://doi.org/10.31971/24500267.19.18
12. Polkowski P., *Bezzałogowe statki powietrzne*, Rocznik Bezpieczeństwa Międzynarodowego, 10(1), 2016, s. 237-248. https://doi.org/10.34862/rbm.2016.1.16
13. Rochowicz R., *Drony w wojnie Ukrainy z Rosją*, Problemy Techniki Uzbrojenia, 160(2), 2022, s. 97-117. https://doi.org/10.5604/01.3001.0015.9900
14. Sitkiewicz A., Karcz K., *Zagrożenia bezpieczeństwa systemów teleinformatycznych w obszarze infrastruktury krytycznej w przestrzeni kosmicznej*, [w:] *Polacy o Kosmosie. Sektor kosmiczny w perspektywie prawa, polityki i bezpieczeństwa*, red. nauk. M. Jabłoński, M. Ulański, Z. Popowicz, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń 2024, s. 140
15. Świeczkowski M., *Technologiczna odpowiedź struktur bezpieczeństwa portu na zagrożenia ze strony bezzałogowych statków powietrznych*, Rocznik Bezpieczeństwa Morskiego rok XIII, Akademia Marynarki Wojennej im. Bohaterów Westerplatte, Gdynia 2019.

16. Terebecki M., *Wykorzystanie nowoczesnych technologii przez wojska obrony terytorialnej podczas działań - roje dronów*, Zeszyty Naukowe Pro Publico Bono, nr 1, 2022, s. 15-33. https://doi.org/10.5604/01.3001.0016.1956

Netografia

1. *Bayraktar - Ukrainian War Song* (English subtitles, napisy polskie and other languages), 23.05.2022, portal youtube.com, https://www.youtube.com/watch?v=S3FGWPMjl6M.
2. *Bezzałogowce BAYRAKTAR TB2*, portal gov.pl, https://www.gov.pl/web/obrona-narodowa/bezzalogowce-bayraktar-tb2.
3. *Bóbr dalekiego zasięgu, czyli czym Ukraińcy bombardują Rosję*, 22.01.2024, portal rp.pl, https://www.rp.pl/konflikty-zbrojne/art39728931-bobr-dalekiego-zasiegu-czyli-czym-ukraincy-bombarduja-rosje.
4. Dąbrowski M., *MSPO 2019: Elektromagnetyczne Lance przeciwko dronom*, 06.09.2019, portal defence24.pl, https://defence24.pl/przemysl/mspo-2019-elektromagnetyczne-lance-przeciwko-dronom.
5. *DIRECTORY. Tactics of use by the enemy FPV drones (in diagrams) and ways to counteract it*, November 9, 2024, Portal Defcad, https://defcad.com/library/tactics-of-using-fpv-drones-by-the-enemy-in-diagrams-and-methods-of-counteraction-eng/.
6. Ditrich R., *Sceny jak z Gwiezdnych Wojen. Tak Ukraina walczy z bezzałogowcami Geran-2*, 06.11.2024, portal forsal.pl, https://forsal.pl/swiat/ukraina/artykuly/9669711,sceny-jak-z-gwiezdnych-wojen-tak-ukraina-walczy-z-bezzalogowcami-gera.html.
7. Gawęda M., *Siły Systemów Bezzałogowych SZU. Jak Ukraina utworzyła wojska dronowe? [ANALIZA]*, 23.11.2024, portal defence24.pl, https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/sily-systemow-bezzalogowych-szu-jak-ukraina-utworzyla-wojska-dronowe-analiza.
8. Górski M., *Zełenski: Ukraina stworzyła nowego drona. Do czego służy Palanycia?*, 25.08.2024, portal defence24.pl, https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/zelenski-ukraina-stworzyla-nowego-drona-do-czego-sluzy-palanycia.
9. Juraszek P., *Pierwszy AHS Krab zniszczony w walce. Dokonał tego rosyjski Spec-naz*, 28 listopada 2022 r., portal wp.pl, https://tech.wp.pl/pierwszy-ahs-krab-zniszczony-w-walce-kulisy-brutalnej-wojny-artyleryjskiej,6838782676957888a.
10. Juraszek P., *Rosjanie zaatakowali Shahedami. Miały nawigację ze sprzętu rolniczego*, 03.01.2025, portal tech.wp.pl, https://tech.wp.pl/rosjanie-zaatakowali-shahedami-miały-nawigacje-ze-sprzetu-rolniczego,7110275941415680a.
11. Kozubel M., *Nowy ukraiński system WRE przeciwko dronom przyjęty na uzbrojenie*, 11.11.2023, portal defence24.pl, https://defence24.pl/wojna-na-ukrainie--raport-specjalny-defence24/nowy-ukrainski-system-wre-przeciwko-dronom-przyjety-na-uzbrojenie.
12. *Marynarka Wojenna Ukrainy ujawniła szczegóły o zestrzeleniu irańskiego drona nad Morzem Czarnym*, 06.06.2023, portal mil.in.ua, https://mil.in.ua/pl/news/

marynarka-wojenna-ukrainy-ujawnila-szczegoly-o-zestrzeleniu-iranskiego-drona-nad-morzem-czarnym/.
13. Mielczarek F., *Fenomen rosyjskich superdronów Lancet. Zaskakują Ukraińców*, 30 sierpnia 2023 r., portal geekweek.interia.pl, https://geekweek.interia.pl/militaria/news-fenomen-rosyjskich-superdronow-lancet-zaskakuja-ukraincow,nId,6995209.
14. Mielczarek F., *Ukraiński wywiad w końcu ujawnił swoją tajną broń*, 17.11.2023, portal geekweek.interia.pl, https://geekweek.interia.pl/lotnictwo/news-ukrainski-wywiad-w-koncu-ujawnil-swoja-tajna-bron,nId,7155614.
15. Mitkow M., *Systemy antydronowe - konieczność na dzisiejszym polu walki [ANALIZA]*, 19.09.2023, portal defence23.pl, https://defence24.pl/przemysl/systemy-antydronowe-koniecznosc-na-dzisiejszym-polu-walki-analiza.
16. Mitkow M., *Widziane z orbity: rosyjski magazyn dronów Shahed zniszczony*, 25.06.2024, portal space24.pl, https://space24.pl/satelity/obserwacja-ziemi/widziane-z-orbity-rosyjski-magazyn-dronow-shahed-zniszczony.
17. Muczyński R., *Palanycia – pocisk-bezzałogowiec w Siłach Zbrojnych Ukrainy*, 26.08.2024, portal milmag.pl, https://milmag.pl/palanycia-pocisk-bezzalogowiec-w-silach-zbrojnych-ukrainy.
18. *Największy atak od początku agresji. Rosja wysłała ponad 250 dronów*, 2.02.2024, portal tvn24.pl, https://tvn24.pl/swiat/ukraina-najwiekszy-atak-od-poczatku-agresji-rosja-wyslala-ponad-250-dronow-st8318858.
19. *„Nie ma już zakładu w Riazaniu". Pożar i zniszczenia po ataku dronów*, 24.01.2025, portal money.pl, https://www.money.pl/gospodarka/nie-ma-juz-zakladu-w-riazaniu-pozar-i-zniszczenia-po-ataku-dronow-7117604861647648a.html.
20. *Rodzaje dronów FPV*, 26.07.2022, portal wgoglach.pl, https://wgoglach.pl/rodzaje-dronow-fpv/.
21. *Rosjanie zaczęli używać dronów kamikadze Shahed-131*, 14.10.2022, portal mil.in.ua, https://mil.in.ua/pl/news/rosjanie-zaczeli-uzywac-dronow-kamikadze-shahed-131/.
22. Ruszkiewicz S., *Wojna dronów na froncie. „Rosjanie używają zwykłych składaków"*, 03.02.2025, portal wiadomosci.wp.pl, https://wiadomosci.wp.pl/wojna-dronow-na-froncie-rosjanie-uzywaja-zwyklych-skladakow-7121283399826240a.
23. Strembski M., *Silny atak Rosji na ukraińską infrastrukturę energetyczną*, 26.08.2024, portal portalmilitarny.pl, https://portalmilitarny.pl/wiadomosci/silny-atak-rosji-na-ukrainska-infrastrukture-energetyczna/.
24. Szopa M., *Ile Rosjanie przepłacają za drony Szahid?*, 06.02.2024. portal defence24.pl, https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/ile-rosjanie-przeplacaja-za-drony-szahid.
25. Tetera S., *Lutyj - ukraiński dron strategiczny*, 18.05.2024, portal onet.pl, https://www.onet.pl/informacje/nowa-technika-wojskowa/lutyj-ukrainski-dron-strategiczny/z50psmf,30bc1058.
26. Tomiczek M., *Systemy walki z dronami. Potrzebny sprzęt na takiej wojnie*, 06.01.2024, portal tech.wp.pl, https://tech.wp.pl/systemy-walki-z-dronami-potrzebny-sprzet-na-takiej-wojnie,6981818801076736a.

27. *Ukraina przeprowadziła największy od początku wojny atak dronów na Rosję,* 24.01.2025, portal wiadomosci.onet.pl, https://wiadomosci.onet.pl/najwiekszy-taki-atak-ukrainy-od-poczatku-wojny-174-drony/fvfx3fy.
28. *Wojna w Ukrainie. Zaskakujące ukraińskie naloty na Rosję*, 02.02.2025, portal rp.pl, https://www.rp.pl/konflikty-zbrojne/art41756631-wojna-w-ukrainie-zaskakujace-ukrainskie-naloty-na-rosje.
29. *Wolontariusz Serhij Prytula pokazał drony kamikadze Bóbr*, 30.07.2023, portal mil.un.ua, https://mil.in.ua/pl/news/wolontariusz-serhij-prytula-pokazal-drony-kamikadze-bobr/.
30. *Zastosowanie dronów oraz ich historia*, 02.06.2017, portal megadron.pl, https://megadron.pl/pl/blog/zastosowanie-dronow-oraz-ich-historia-1536843674.html?srsltid=AfmBOoqm6BS8tvNad-qcLSLDuKZ-R8nmZEhma_RwBL4u-GyqvkMTk9CHC.
31. *„Znacznie szybszy i potężniejszy". Ukraina po raz pierwszy użyła nowego drona Palianyca*, 25.08.2024, portal rp.pl, https://www.rp.pl/swiat/art41017351-znacznie-szybszy-i-potezniejszy-ukraina-po-raz-pierwszy-uzyla-nowego-drona-palianyca.

dr Barbara Stefaniuk
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0001-7430-075X
https://doi.org/10.29316/9788368103199_6

CYBERTERRORYZM JAKO ZAGROŻENIE BEZPIECZEŃSTWA GLOBALNEGO

CYBERTERRORISM AS A THREAT TO GLOBAL SECURITY

Streszczenie

Zagrożenie terroryzmem w ujęciu ogólnym postrzegane jest współcześnie jako jedno z największych wyzwań dla bezpieczeństwa globalnego. Nieprzypadkowo więc ta problematyka jest przedmiotem licznych analiz naukowych. Problemy globalne najczęściej postrzegane są w kontekście skali zagrożeń oraz wyzwań, jakie niosą dla ludzkości i świata. Celem niniejszego rozdziału będzie przybliżenie zagrożenia cyberterroryzmem jako zagrożenia bezpieczeństwa globalnego. Cyberterroryzm globalny, może przybierać różne formy oddziaływania na wybrane obszary funkcjonowania państwa i społeczeństwa., które ukierunkowane są na zaatakowanie i całkowite zniszczenie m.in. kluczowych obiektów infrastruktury krytycznej, jak i inżynierii społecznej.

Słowa kluczowe: bezpieczeństwo globalne, zagrożenie, terroryzm, cyberterroryzm, globalizacja

Summary

The threat of terrorism in general is currently perceived as one of the greatest challenges to global security in the modern era. It is no coincidence that this issue is the subject of numerous scientific analyses. Global problems are most often perceived in the context of the scale of threats and challenges they pose to humanity and the world. The aim of this chapter will be to present the threat of cyberterrorism as a threat to global security. Global cyberterrorism can take various forms of impact on selected areas of the functioning of the state and society, which are aimed at attacking and completely destroying, among others, key critical infrastructure facilities, as well as social engineering.

Keywords: global security, threat, terrorism, cyberterrorism, globalization

Wstęp

Współczesny świat podlega niezwykle dynamicznym i ciągłym zmianom, które uwarunkowane są różnymi zagrożeniami. Zagrożenia te mogą przybierać formę zagrożeń globalnych, które mogą mieć wpływ na bezpieczeństwo międzynarodowe i globalne. W związku z rozwojem technologii informacyjnej powstaje wiele form zagrożeń cybernetycznych. Terroryzm, który jest definiowany jako różnie umotywowana i realizowana z naruszeniem porządku prawnego forma przemocy polityczno – społecznej podjęta przez pojedyncze osoby lub grupy osób, skutkująca wywołaniem strat fizycznych, psychicznych lub materialnych[1]. Zagrożenie każdą formą terroryzmu jest obecnie zagrożeniem permanentnym i nie ma możliwości jego całkowitego wyeliminowania. W niniejszym rozdziale autorka skupiła swoją uwagę na zagrożeniu cyberterroryzmem jako jednym z rodzajów terroryzmu, który w pełni można uznać za globalny. Obecnie żyjemy w społeczeństwie sieciowym, które umożliwia korzystanie z dobrodziejstw Internetu w każdej sferze życia. Jednym z najbardziej znaczących zagrożeń dla współczesnej cywilizacji jest zagrożenie cyberterroryzmem. Cyberterroryzm jest to bezprawny atak lub groźba ataku na komputery, sieci lub systemy informacyjne, w celu zastraszenia lub wymuszenia na rządzie lub ludziach daleko idących politycznych i społecznych celów[2].

Gwałtowny postęp technologiczny w elektronice, technologii informacyjnej i telekomunikacji przyczynił się do rozwoju nowych zagrożeń o charakterze cyberterrorystycznym. Współcześnie zagrożenie cyberterroryzmem pozostaje jednym z najważniejszych globalnych wyzwań, z jakimi musi się zmierzyć także Polska oraz służby mundurowe, dbające o bezpieczeństwo państwa. Cyberterroryzm stanowi realne zagrożenie dla życia ludzi, stabilności instytucji państwowych, infrastruktury krytycznej państwa oraz ładu międzynarodowego, a także dla bezpieczeństwa globalnego. Rozwój cyberterroryzmu jest przejawem globalizacji i towarzyszących jej procesów. Globalizacja wpłynęła na cyberbezpieczeństwo, zwiększając złożoność i skalę potencjalnych zagrożeń oraz rozszerzając powierzchnię ataku[3]. Bezpieczeństwo globalne wchodzi w zakres pojęciowy bezpieczeństwa międzynarodowego, które

[1] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*, Wydawnictwo Difin, Warszawa 2017, s. 26.

[2] W. Smolski, *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*. https://www.repozytorium.uni.wroc.pl/dlibra/publication/67850, [dostęp: 29.03.2025].

[3] A. Malewska i M. Filary-Szczepanik*, Globalizacja i współzależność*, Wydawnictwo Naukowe Akademii Ignatianum w Krakowie, Kraków 2022, s. 316.

obejmuje bezpieczeństwo całej zbiorowości państw oraz system międzynarodowy, w jakim państwa te występują. W świetle literatury przedmiotu bezpieczeństwo globalne obejmuje środki wojskowe i dyplomatyczne, które państwa i organizacje międzynarodowe, takie jak Organizacja Narodów Zjednoczonych i NATO, podejmują w celu zapewnienia wzajemnego bezpieczeństwa[4]. Ze względu na skalę zagrożeń i potencjalne skutki dla funkcjonowania państw i społeczeństw, problematyka zagrożeń cyberterroryzmem szybko nabierają znaczenia globalnego i stają się nieodłączną częścią relacji międzynarodowych. W niniejszym rozdziale wykorzystano następujące metody badawcze: analizę porównawczą, analizę i krytykę piśmiennictwa, analizę i krytykę źródeł oraz studium przypadku.

Zagrożenia bezpieczeństwa globalnego

Uwarunkowania zmian w globalnym środowisku bezpieczeństwa wskazują na coraz to bardziej zwiększoną liczbę zagrożeń w nim występujących. Współcześnie poziom bezpieczeństwa nie jest mierzony tylko prawdopodobieństwem wystąpienia zagrożenia militarnego. Cyfryzacja niemal wszystkich dziedzin życia ma niewątpliwie ogromny wpływ na bezpieczeństwo ludzi i państwa w wymiarze globalnym. Powszechne zastosowanie komputerów i technologii teleinformatycznych w sferze publicznej, jak i prywatnej wiąże się z ryzykiem powstania zagrożeń o charakterze cybernetycznym[5]. Zagrożenie jest to odziaływanie czynnika destrukcyjnego na podmiot. Etymologia pojęcia globalny oznacza odnoszący się do całego świata[6]. Zagrożenia globalne to takie, których nie można rozwiązać w skali tylko jednego państwa lub grupy państw. Dotyczą bowiem całej ludzkości, jej trwania i rozwoju. Wśród nich ważne miejsce zajmują zagrożenia dla środowiska naturalnego, dotyczące zmiany klimatu, przekształcanie się gleb w pustynie, brak dostępu do wody pitnej, zanieczyszczenie powietrza, wycinanie lasów tropikalnych lub nadmierna eksploatacja zasobów naturalnych. Równie istotne są problemy rozwoju na świecie – ubóstwo, niedożywienie, brak dostępu do leków i edukacji oraz problemy polityczne – rosnąca skala migracji, konflikty wewnętrzne

[4] R. Kuźniar, *Bezpieczeństwo międzynarodowe, Wydanie drugie rozszerzone*, Wydawnictwo naukowe Scholar, Warszawa 2022.

[5] T. Zieliński, P. Mróz, R. Bartnik, *Bezpieczeństwo i obrona Unii Europejskiej*, Akademia Sztuki Wojennej, Warszawa 2020, s. 43.

[6] *Globalny*, słownik PWN, https://sjp.pwn.pl/slowniki/globalny.html, [dostęp: 28.03.2025].

i międzynarodowe. Szczególną uwagę należy zwrócić na zagrożenie terroryzmem[7], który może przybrać postać cyberterroryzmu globalnego i rozwoju związanych z nim cyberzagrożeń.

Charakterystyka wybranych cyberzagrożeń

Wraz z rozwojem cyberzagrożeń podmioty, które próbują zagrozić bezpieczeństwu cybernetycznemu państwa lub organizacji, stają się coraz bardziej zróżnicowane. Cyberterroryści mogą pochodzić z kręgów zorganizowanych grup przestępczych, użytkowników wewnętrznych, operatów usług, haktywistów a nawet organów wywiadu wspieranych przez określone państwa[8]. Współczesne systemy i sieci informatyczne można atakować w różny sposób, którego efektem będzie osiągnięcie jednego z niszczycielskich celów, mianowicie: utrata danych, kradzież danych, ujawnienie danych, zdyskredytowanie danych, destabilizacja infrastruktury krytycznej, przejęcie kontroli nad systemem lub całym środowiskiem, szantaż lub awaria systemu[9]. Najgroźniejszą formą zagrożenia informatycznego jest cyberterroryzm, który definiowany jest jako politycznie umotywowany atak bądź groźba ataku na komputery, systemy lub sieci informacyjne. Jego celem jest doprowadzenie do zniszczenia infrastruktury oraz zastraszenie lub wymuszenie na rządach i ludziach określonych politycznych, bądź społecznych działań[10]. Wszelkie cyberzagrożenia mają swoje miejsce w cyberprzestrzeni. W świetle literatury przedmiotu cyberprzestrzeń jest pojmowana jako byt wirtualny, pozbawiony parametru geograficznego, jest niemierzalny i nieograniczony[11]. W. Krztoń określa cyberprzestrzeń jako globalną domenę środowiska informacyjnego, składającą się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe,

[7] *Globalizacja – szanse i zagrożenia*, https://globalna.ceo.org.pl/materialy/globalizacja-szanse-i-zagrozenia/, [dostęp: 24.03.2025].

[8] M., Rytko-Marczewska, *Haktywizm (Cyberterroryzm, Haking, Protest obywatelski, Cyberaktywizm, E- Mobilizacja)*, Wydawnictwo UMCS Lublin, Lublin 2014.

[9] T. Zieliński, P. Mróz, R. Bartnik, *Bezpieczeństwo i obrona Unii….,* op. cit., s. 45.

[10] Ibidem.

[11] A. Gałecki, *Bezpieczeństwo informacji w dobie cyberprzestrzennych zagrożeń*, Wydawnictwo Wyższa Szkoła Bezpieczeństwa, Poznań 2021, s. 51.

a także osadzone w nich procesory i kontrolery[12]. Cyberprzestrzeń to wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery z całego świata[13]. Cyberataki mogą występować w postaci samodzielnego ataku np. na systemy odpowiedzialne za kontrolę ruchu lotniczego lub funkcjonowanie bankowości elektronicznej, co ma na celu spowodowanie jego dysfunkcyjności. Cyberataki mogą mieć również formę złożonych operacji i spowodować rolę wspierającą podczas zamachu fizycznego np. wyłączenie kontroli dostępu w obiekcie lub blokadę komunikacji pomiędzy służbami. Inną formą ataku terrorystycznego może być technika zamachu prowadzonego w cyberprzestrzeni za pomocą pozyskiwania informacji[14]. Działalność służb wywiadowczych jest bardzo ważna w procesie pozyskiwania informacji, ponieważ przyczynia się do zapobiegania i zwalczania czynów zagrażających ujawnieniem tajemnicy państwowej, przyczynia się do zapobiegania i zwalczania przestępczości związanej z funkcjonowaniem technologii informacyjnej i komunikacyjnej[15].

Zagrożenia cybernetyczne można podzielić na cztery główne kategorie, do której zalicza się cyberprzestępczość, cybernetyczne szpiegostwo, cyberterroryzm i cyberwojnę[16].

Cyberprzestępczość to wszelkie działania przeciwko poufności, integralności i dostępności danych, dotyczących nielegalnego dostępu do systemów to: hacking, podsłuch, podawanie fałszywej tożsamości, szpiegostwo komputerowe, sabotaże oraz wymuszenia komputerowe. Do cyberprzestępczości zaliczyć można wirtualne przestępstwa finansowe, bankowe, a więc newralgiczne systemy infrastruktury państwa.

Cyberprzestępstwa[17], to działania przeciwko poufności, integralności i dostępności danych, dotyczących nielegalnego dostępu do systemów obej-

[12] J. Lebiedź, W. Krztoń, B. Stefaniuk, *Współczesne wyzwania bezpieczeństwa narodowego. Zarządzanie kryzysowe. Wojna w cyberprzestrzeni. Rzeczywistość wirtualna*, Wydawnictwo Texter, Warszawa 2018, s. 100-101.

[13] Ibidem.

[14] J. Stelmach, *Zamachy terrorystyczne. Istota i koncepcja reagowania*, Wydawnictwo Difin, Warszawa 2023, s. 164.

[15] A. Olech*, Walka z terroryzmem polskie a francuskie doświadczenie*, Wydawnictwo Difin, Warszawa 2021.

[16] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*, Wydawnictwo Difin, Warszawa 2017, s. 52.

[17] P. Różański, A. Warmiński., H. Chałupczak, *Zagrożenia bezpieczeństwa i porządku publicznego we współczesnej Polsce (wybrane aspekty),* Akademia Wychowania Fizycznego Józefa Piłsudskiego w Warszawie, Wydział Wychowania Fizycznego i zdrowia w Białej Podlaskiej, Biała Podlaska 2023.

mujące: hacking, podsłuchiwanie i podawanie fałszywej tożsamości, szpiegostwo komputerowe, sabotaże oraz wymuszenia komputerowe:

- manipulacje fakturami lub kontami firmowymi, nieprawdziwe aukcje czy nielegalne używanie kart kredytowych, komputerowe podróbki, molestowanie dzieci czy cyberstalking;
- ataki na życie ludzkie, manipulowanie systemami szpitalnymi lub kontrolą ruchu
- powietrznego, przestępstwa obejmujące dziecięcą pornografię, przekazywanie instrukcji zachowań przestępczych, oferty popełniania przestępstw, molestowanie i lobbing poprzez sieć, rozpowszechnianie fałszywych informacji oraz internetowy hazard;
- przestępstwa powiązane z naruszeniem prawa autorskiego i praw pokrewnych, do których należy np. nieautoryzowanie, kopiowanie i rozpowszechnianie programów komputerowych, cyberprzestępstwa są najczęściej formami przestępstw i działań zabronionych.

Do pierwszej grupy zalicza się oszustwa i fałszerstwa, do drugiej należą: pozyskiwanie, wytwarzanie, rozpowszechnianie oraz posiadanie treści nielegalnych. Trzecią grupą są ataki cybernetyczne na systemy informatyczne, zaś czwartą grupę stanowi kopiowanie i rozpowszechnianie w celach zarobkowych utworów chronionych prawem autorskim.

Cybernetyczne szpiegostwo to rodzaj cyberataku, w którym nieautoryzowany użytkownik próbuje uzyskać dostęp do poufnych lub tajnych danych albo własności intelektualnej (IP) w celu uzyskania korzyści ekonomicznych, przewagi konkurencyjnej lub z powodów politycznych. Szpiegostwo komputerowe to udzielenie obcemu wywiadowi wiadomości, ich gromadzenie lub przechowywanie, włącznie się do sieci komputerowej w celu ich uzyskania lub zgłaszanie gotowości działania na rzecz obcego państwa przeciwko Rzeczypospolitej Polskiej[18]. W sieci zdecydowana większość informacji jest jawna oraz możliwa do skopiowania i wykorzystania. Jednak niektóre nie są jawne, do których zalicza się: niejawne informacje wojskowe, tajemnice handlowe czy dane osobowe. To właśnie one stanowią obszar zainteresowań terrorystów[19]. W literaturze przedmiotu istnieje wiele pojęć cyberterroryzmu. Cyberterroryzm to wykorzystywanie cyberprzestrzeni w działaniach terrorystycznych. Narzędziem do wykonywania aktów terroru jest sieć komputerowa, a celem

[18] art. 130 Ustawy z dnia 6 czerwca 1997 r. *Kodeks Karny* (Dz. U. 1997 Nr 88, poz. 553).

[19] S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki- organizacji- państwa,* Wydawnictwo CedeWu, Warszawa 2016, s. 210.

zasoby infrastruktury krytycznej. Przejęcie kontroli nad tymi zasobami, które sterowane są za pomocą komputerów i Internetu, powoduje chaos i panikę oraz brak stabilizacji w funkcjonowaniu państwa[20].

Cyberwojna to jeden z elementów wojny informacyjnej. W cyberwojnie głównymi celami są szpiegostwo i sabotaż[21]. Wielu ekspertów ocenia, że w praktyce oznacza ona cyberterroryzm: ataki na infrastrukturę IT lub infrastrukturę sieciową na terenie wrogiego państwa. Na celownik brane są instytucje publiczne oraz firmy prywatne. Innym przejawem cyberwojny są akcje internetowych trolli, którzy tworzą, a następnie kolportują fake newsy np. w mediach społecznościowych. Dla agresora celem w cyberwojnie jest zmuszenie przeciwnika do posłuszeństwa. Wojna cybernetyczna jest narzędziem, żeby narzucić swoją wolę innemu państwu. Przykładem wojny cybernetycznej może być atak na systemy wyborcze lub blokowanie serwerów www. J. Kuck prezentuje następującą klasyfikację zagrożeń występujących w cyberprzestrzeni, dzieląc je na siedem kategorii[22]:

- stealingpasswords – uzyskiwanie haseł dostępu do sieci,
- social engineering – wykorzystanie niekompetencji osób posiadających dostęp do
- systemu,
- bugs and backdoors – nielegalne korzystanie z systemu lub używanie nielegalnego
- oprogramowania,
- authenticationfailures – zniszczenie mechanizmu autoryzacji,
- protocolfailures – wykorzystanie luk w oprogramowaniu i systemach,
- information leakage – przechwycenie informacji dostępnych dla administratora,
- denial of service – blokada kont użytkowników systemu.

Obszar działań cyberterrorystów jest bardzo obszerny, trudny do jednoznacznego zidentyfikowania i ciągle powiększający swój zasięg na nowe obszary. W związku z coraz częstszym użytkowaniem urządzeń mobilnych

[20] M. Górka, *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku,* Wydawnictwo Difin, Warszawa 2014, s. 265.

[21] M. Marszycki, *Cyberwojna między Rosją a Ukrainą wciąż trwa*, 3 marca 2023 r., https://itwiz.pl/cyberwojna-miedzy-rosja-a-ukraina-wciaz-trwa, [dostęp: 30.03.2025].

[22] J. Kuck, *Bezpieczeństwo informacyjne. Cyberterroryzm. Przestępczość komputerowa*, Wydawnictwo Państwowej Akademii Nauk Stosowanych w Jarosławiu, Jarosław 2023, s. 109-110.

wzrasta poziom ich zagrożeń, które można zaobserwować poprzez zwiększanie się ilości złośliwych programów wykrywanych na urządzeniach mobilnych. Do najczęściej stosowanych kategorii cyberzagrożeń przez cyberprzestępców w ostatnich latach należą m.in.[23]:

- ataki odmowy usługi, które są nakierowane na zaburzenie działania systemów i usług poprzez wyczerpanie ich zasobów, najczęściej spotykany przypadek Distributed Denial of Service (DDoS) osiąga ten cel poprzez przeciążenie wybranej usługi zapytaniami wysyłanymi z wielu kontrolowanych urządzeń naraz;
- ataki ransomware, w których cyberprzestępca szantażuje organizację po przejęciu kontroli nad jej zasobami, żąda okupu pod różnymi warunkami, na przykład przywrócenia dostępności danych i systemów lub obietnicy nieudostępniania przejętych wrażliwych informacji publicznie, odnotowano też przypadki żądania okupu za przerwanie ataku odmowy usługi, które nazywa się Ransom Denial of Service (RDoS)[24];
- ataki na dane, w ramach których dochodzi do nieuprawnionego dostępu do poufnych danych, może być to kradzież danych spowodowana celowo w ramach cyberataku lub nieumyślny wyciek w wyniku błędu.

Kolejnym rodzajem cyberzagrożenia jest socjotechnika mająca zastosowanie w inżynierii społecznej. To każda metoda, mająca na celu oszukanie człowieka do uzyskania dostępu do systemu lub danych. Warto podkreślić, że nie chodzi tu wyłącznie o maile phishingowe, ale złośliwe połączenia głosowe, smsy, kody QR, podstawienie strony bankowej[25]. Popularnym wektorem ataku jest obecnie Business Email Compromise (BEC), w którym atakujący podszywają się pod zaufaną osobę (np. prezesa, księgową) w celu wyłudzenia pieniędzy, na przykład wywierając presję do uregulowania płatności pod wskazanym adresem bankowym.

Złośliwe oprogramowanie jako ogólna kategoria, opisująca wszelkie ataki wykorzystujące złośliwy kod, programy i aplikacje do osiągnięcia swojego celu. Obecnie zauważyć można dużą popularność tzw. infostealerów, czyli oprogramowania do kradzieży danych z zainfekowanego urządzenia. Znalezienie poświadczeń pracownika organizacji w opublikowanych w Internecie

[23] M. Marczyk, M. Stolarz, B. Terebiński, *Bezpieczeństwo działań w cyberprzestrzeni. Wybrane aspekty. Tom II Działania w cyberprzestrzeni,* Akademia Sztuki Wojennej, Warszawa 2022, s. 184.

[24] Ibidem.

[25] J. Kuck, *Bezpieczeństwo informacyjne. Cyberterroryzm. Przestępczość*…, op. cit., s. 109.

logach takiego programu jest jedną z częstszych metod inicjalnego dostępu do organizacji[26].

Manipulacja informacją w sieci cyfrowej na celu wywołanie określonego wpływu na wydarzenie lub proces polityczny. Jest to szeroka kategoria działań, mieszcząca w sobie praktyki takie jak, dezinformacja i propaganda w sieciach i serwisach społecznościowych.

Istnieje kilka rodzajów ataków wykorzystujących inżynierię społeczną, takich jak wyłudzanie informacji, wyłudzanie informacji przez SMS, wyłudzanie informacji przez telefon i pretekst. Wyłudzanie informacji zwykle odbywa się za pośrednictwem poczty e-mail. Cyberprzestępca wysyła wiadomość e-mail wyłudzającą informacje z linkiem albo załącznikiem przeznaczonym do kliknięcia lub pobrania przez ofiarę. Kliknięcie lub pobranie podejrzanego linku albo załącznika może spowodować pobranie złośliwego oprogramowania na urządzenie ofiary i kradzież jej prywatnych danych przez cyberprzestępcę. Wyłudzanie informacji przez telefon i wyłudzanie informacji przez SMS są odmianami wyłudzania informacji różniącymi się wykorzystywaną metodą komunikacji.

Cyberterroryzm – jako forma terroryzmu globalnego

Od najdawniejszych lat rozwój technologiczny w znaczący sposób wpływał na życie człowieka. W ostatnich latach szczególnie intensywnie rozwija się obszar informatyki oraz szerokopasmowego Internetu, co przekłada się niewątpliwie na zwiększenie liczby jego użytkowników. Codzienne funkcjonowanie jest już nierozerwalnie związane z cyberprzestrzenią, czyli przestrzenią wirtualną, która stwarza warunki do rozwoju nowej platformy walki zbrojnej, nowej formy terroryzmu – cyberterroryzmu. Przestrzeń wirtualna może być określana jako globalna wioska, świat, w którym ludzie, dzięki środkom masowego przekazu, przeżywają jednocześnie te same wydarzenia i używają tych samych produktów masowej konsumpcji[27]. Zdefiniowanie cyberterroryzmu nie jest sprawą prostą, ponieważ obszar działań cyberterrorystów jest dość szeroki i trudny do jednoznacznego określenia. W literaturze przedmiotu istnieje wiele definicji cyberterroryzmu. Zjawisko cyberterroryzmu jest bardzo zróżnicowane, co przejawia się jego dynamiką. Cyberterroryzm jest

[26] Ibidem.

[27] *Globalny*, słownik PWN, https://sjp.pwn.pl/slowniki/globalny.html, [dostęp: 28.03.2025].

to jedna z form terroryzmu[28]. Ponadto, występuje pod wieloma postaciami, które zmieniają się pod wpływem rozwoju cywilizacyjnego i technologicznego. Cyberterroryzm w zakresie funkcjonowania infrastruktury krytycznej jest działaniem, które hamuje i całkowicie blokuje działanie systemów komputerowych, aby osiągnąć konkretne cele terrorystyczne[29].

Cyberterroryzm - pojęcie to odnosi się do bezprawnych ataków i zagrożeń wobec komputerów, sieci i informacji przechowywanych w nich, celem których jest zastraszenie lub zmuszenie rządu albo jego ludzi, po to, aby osiągnąć pewne korzyści polityczne lub społeczne[30].

Pojęcie cyberterroryzmu używane jest w kontekście politycznie umotywowanego ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów w szerokim rozumieniu tego słowa[31]. Cyberterroryzm może być wiązany z działaniami podejmowanymi przez rozmaite organizacje terrorystyczne z użyciem sieci internetowej, której celem jest zakłócenie pracy sieci komputerowych, wywołanie przez to chaosu i paniki wśród ludzi[32]. Cyberterroryzm ma miejsce wówczas, gdy[33]:

- jest przeprowadzony z wykorzystaniem systemów transmisji danych,
- skutkuje zniszczeniami i dalszymi działaniami przeciwko innym osobom,
- jest wymierzony przeciwko komputerom, sieciom oraz bazom danych, kontrolowanym przez instytucje rządowe,
- wywołuje chaos i panikę,
- doprowadza do zagrożenia życia i zdrowia ludzi,
- prowadzi do eksplozji
- skutkuje znacznymi stratami finansowymi,
- jest wymierzony w elementy infrastruktury krytycznej państwa.

---

[28] M. Górka, *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa 2014, s. 282.

[29] J. Stelmach, *Bezpieczeństwo terrorystyczne obiektów użyteczności publicznej,* Tom IV, Wydawnictwo Difin, Warszawa 2022, s. 95.

[30] *Infrastruktura krytyczna na celowniku hakerów – czy można ją skutecznie zabezpieczyć?* 12.02.2025, https://rocznikbezpieczenstwa.pl/ojs/index.php/rbm/article/view/449/404, [dostęp: 29.03.2025].

[31] M. Marczyk, M. Stolarz, B. Terebiński, *Bezpieczeństwo działań w cyberprzestrzeni. Wybrane aspekty. Tom I Działania w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2022.

[32] A. Gałecki*, Bezpieczeństwo informacji w dobie cyberprzestrzennych zagrożeń*, Wydawnictwo Wyższa Szkoła Bezpieczeństwa, Poznań 2021, s. 69.

[33] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny*…, op. cit., s. 52.

Cyberterroryzm to terroryzm dokonywany, planowany i koordynowany w cyberprzestrzeni za pomocą komputerów podłączonych do sieci[34]. Cyberterroryzm to również forma współczesnej wojny, którą cechują przede wszystkim niskie koszty działalności. Do przeprowadzenia ataku nie jest wymagane posiadanie specjalistycznego sprzętu. Cyberterroryści dysponują jedynie komputerem oraz siecią internetową. Cyberterrorystów cechuje wysoki stopień anonimowości[35]. Wśród sprawców cyberataków wyróżnić można trzy główne grupy[36]:

- państwowi hakerzy, którzy działają na zlecenie rządów, którzy wykorzystują cyberataki do destabilizacji strategicznych obiektów lub prowadzenia działań szpiegowskich;
- zorganizowane grupy cyberprzestępcze zmotywowane korzyściami finansowymi, stosujące ataki w celu wymuszenia okupu lub kradzieży danych;
- cyberterroryści, których działania mają na celu wywołanie chaosu i zakłócenie funkcjonowania instytucji publicznych oraz przedsiębiorstw. Cyberterroryści wykorzystują platformy i technologie internetowe do rekrutacji, szkolenia, radykalizacji postaw, publicznej prowokacji, propagandy lub w celu planowania, przygotowywania i przeprowadzania ataków terrorystycznych. Zjawisko to wciąż ewoluuje wraz z pojawianiem się nowych platform i usług, umożliwiając terrorystom znajdowanie nowych i innowacyjnych sposobów wykorzystywania możliwości, jakie zapewniają te technologie.

Najczęstszą formą ataku cyberterrorystów na cele infrastruktury krytycznej jest wysłanie do systemów komputerowych wirusów, które uniemożliwiają ich prawidłowe działanie. Rezultatem takiego działania może być np.: utrata kontroli nad systemem, brak komunikacji, czy nawet konieczność wyłączenia systemów. Czynnikiem wzmacniającym działania terrorystów jest wprowadzany przez nich chaos informacyjny, podsycany publikowaniem fałszywych informacji na stronach internetowych. W dobie globalizacji i rozwoju technologicznego poszczególne obiekty infrastruktury krytycznej są

[34] J. Kuck, *Bezpieczeństwo informacyjne. Cyberterroryzm. Przestępczość komputerowa,* Wydawnictwo Państwowej Akademii Nauk Stosowanych w Jarosławiu, Jarosław 2023, s. 105.

[35] J. Stelmach, *Bezpieczeństwo terrorystyczne obiektów użyteczności*,…, op. cit., s. 95.

[36] *Infrastruktura krytyczna na celowniku hakerów – czy można ją skutecznie zabezpieczyć?* 12.02.2025, https://academy.asseco.pl/learning-center/infrastruktura-krytyczna-na-celowniku-hakerow-czy-mozna-ja-skutecznie-zabezpieczyc/, [dostęp: 28.03.2025].

coraz bardziej od siebie współzależne, nie tylko wymiarze funkcjonowania jednego państwa, ale w wymiarze globalnym. Połączenia sieci transkontynentalne powodują, że skutki ewentualnych zakłóceń mogą mieć swój wymiar globalny. Każdy obiekt infrastruktury może być obiektem ataku terrorystycznego. Jedną z najważniejszych cech współczesnego terroryzmu w każdej jego formie jest jego nieprzewidywalność, co do jego formy, czasu i miejsca, użytych środków i skutków[37]. Cyberatakami zagrożone są wszystkie elementy infrastruktury krytycznej, które funkcjonują dzięki technologii informacyjnej. Obszar zagrożeń cyberterrorystycznych obejmuje m.in.[38]:

Systemy wojskowe – które przechowują informacje o położeniu satelitów, rozmieszczeniu wojsk oraz broni, prowadzących badania nad nowymi rodzajami broni i systemami łączności.

Systemy przedsiębiorstw – które przechowują informacje ważne z punktu widzenia działalności firmy, np.: informacje o rezerwacjach, o klientach, o wykorzystywanych technologiach.

Systemy infrastruktury krytycznej tj.: bankowe, finansowe, energetyczne, telekomunikacyjne, dostarczania wody, transportu, służb do działań w sytuacjach wyjątkowych, które przechowują informacje ważne dla bezpieczeństwa państwa.

Systemy ratownicze – realizujące zadania w zakresie ochrony życia i zdrowia np. szpitale, jednostki organizacyjne systemu ochrony zdrowia, np. Państwowe Ratownictwo Medyczne, Lotnicze Pogotowie Ratunkowe.

Systemy transportowe – drogowe, kolejowe, morskie, lotnicze.

Systemy gazowe – rafinerie, koncerny energetyczne i ciepłownicze.

Zagrożenia w cyberprzestrzeni na infrastrukturę krytyczną mają na celu blokowanie dostępu do systemu informatycznego organizacji, włamanie do systemu lub jego całkowite zniszczenie.

Wybrane metody ataków cybernetycznych

Sieć internetowa i infrastruktura komputerowa wykorzystywane są w bezpośrednich cyberatakach oraz jako podstawowe narzędzia do jego przeprowadzenia. W wyniku rozwoju technologii informacyjnej stale wzrastają

[37] J. Stelmach, *Bezpieczeństwo terrorystyczne obiektów użyteczności publicznej,* Tom IV, Wydawnictwo Difin, Warszawa 2022, s. 93.

[38] A. Gałecki, *Bezpieczeństwo informacji w dobie cyberprzestrzennych zagrożeń*, Wydawnictwo Wyższa Szkoła Bezpieczeństwa, Poznań 2021, s. 73-74.

metody jego przeprowadzenia. Do najczęściej stosowanych metod cyberataków należą m.in.[39]:

- robak – to działanie polegające na zainstalowaniu złośliwego oprogramowania samoreplikującego niszczące dane,
- cookies – to technika polegająca na zbieraniu informacji o użytkownikach komputerów,
- phishing – to metoda oparta głównie na inżynierii społecznej, polegającej na podszywaniu się pod instytucje celem kradzieży danych,
- exploit – to użycie złośliwego oprogramowania, pozwalającego na bezpośredni dostęp do komputera ofiary,
- hijacking – obejmuje przechwycenie transmisji danych pomiędzy dwoma komputerami,
- inżynieria społeczna – to atak wykorzystujący niekompetencję i niewiedzę osób w zakresie działania systemów komputerowych,
- spam – polegający wysyłaniu na konto pocztowe atakowanego dużej ilości niechcianych wiadomości tekstowych,
- spoofing – to podszycie się pod urządzenie w sieci, w celu dokonania włamania do systemu,
- ransomware – to forma złośliwego oprogramowania, która blokuje użytkownika z jego plików lub urządzenia, a następnie żąda zapłaty za przywrócenie dostępu, atakujący ransomware uderzają w firmy, organizacje oraz indywidualnych użytkowników[40].

W ostatnim czasie obserwujemy tendencję do podejmowania w niej działań stricte operacyjnych atakowanie sieci teleinformatycznych i systemów technologicznych, mających strategiczne znaczenie dla bezpieczeństwa państwa. Warto podkreślić, że ataki cybernetyczne i operacje na szerszą skalę mogą podejmować zarówno grupy przestępcze, terrorystyczne, jak i państwa, w ramach szeroko rozumianej wojny informacyjnej. Z pewnością można stwierdzić, że wszystkie rodzaje niebezpieczeństw istniejących w tradycyjnej, fizycznej geoprzestrzeni będą mieć swoje odpowiedniki w cyberprzestrzeni.

[39] J. Kuck*, Bezpieczeństwo informacyjne. Cyberterroryzm. Przestępczość*…, op. cit., s. 75-77.

[40] M. Marczyk, M. Stolarz, B. Terebiński, *Bezpieczeństwo działań w cyberprzestrzeni. Wybrane aspekty. Tom II...,* op. cit., s. 82-84.

Charakterystyka wybranych ataków cybernetycznych na infrastrukturę krytyczną – studium przypadku

Do podmiotów dokonujących ataków cyberterrorystycznych należy zaliczyć zorganizowane grupy lub osoby działające indywidualnie. Wskazując na zagrożenia infrastruktury krytycznej można wyróżnić obiekty, instytucje oraz systemy wykorzystujące transmisję informacji w cyberprzestrzeni. Przykładem cyberterroryzmu na systemy infrastruktury krytycznej jest cyberatak na Lotnicze Pogotowie Ratunkowe w Polsce. W lutym 2022 r. celem cyberataku stało się Lotnicze Pogotowie Ratunkowe. Mimo informatycznego zamachu ani jeden dyżur nie został zawieszony, wszystkie wezwania do misji ratunkowych i transportów międzyszpitalnych były na bieżąco realizowane. Przez ponad tydzień po ataku cyberprzestępców jednostki Lotniczego Pogotowia Ratunkowego w całym kraju były pozbawione możliwości korzystania ze swoich systemów komputerowych. Niedostępne były systemy kluczowe dla działania pogotowia, jak system przesyłania informacji o prowadzonych interwencjach, strona www i poczta elektroniczna. Hakerzy zażądali okupu w wysokości 390 tysięcy dolarów, czyli około 1,5 mln złotych[41]. Najnowszym i najlepszym przykładem cyberterroryzmu jest eskalacja agresji Rosji na Ukrainę z lutego 2022 roku, która zapoczątkowała nowy etap rozwoju stosunków międzynarodowych i bezpieczeństwa globalnego[42]. Od początku wojny w Ukrainie w zasadzie możemy mówić o ciągłych, nieustających cyberoperacjach w postaci ataków na sieci i systemy informatyczne, cyberszpiegostwie oraz operacjach psychologicznych i informacyjnych radykalizujących społeczeństwo. Rosyjskim cybernetycznym "przygotowaniem ogniowym" w kierunku Ukrainy była m.in. masowa podmiana stron ukraińskich urzędów, wysyłanie fałszywych maili/sms-ów oraz ataki DDoS na witryny wojskowe, urzędowe oraz bankowe, portale informacyjne i dostawców usług internetowych. Rząd ukraiński zaapelował do podziemia hakerskiego o odpowiedź. Właściciel ukraińskiej firmy Cyber Unit Technologies wyznaczył nagrodę: 100 tys. dolarów za włamanie do rosyjskich systemów IT. Do ataku na rosyjskie

[41] M. Stańczyk, K. Lechowicz-Dyl, *Cyberatak na Lotnicze Pogotowie Ratunkowe. Hakerzy zażądali 390 tys. dolarów okupu*, PAP, 21 lutego 2022 r., https://www.pap.pl/aktualnosci/news%2C1086018%2Ccyberatak-na-lotnicze-pogotowie-ratunkowe-hakerzy-zazadali-390-tys-dolarow, [dostęp: 29.03.2025].

[42] R. Panas, *Wojna cybernetyczna i cyberterroryzm – czym są? Czy Polsce grozi cyberwojna?* 10 marca 2022 r., https://nano.komputronik.pl/n/cyberwojna-cyberterroryzm-wojna-cybernetyczna/, [dostęp: 29.03.2025].

serwery ruszyła też międzynarodowa grupa Anonymous. Większość rosyjskich cyberataków skierowana była na agencje wojskowe i rządowe oraz na infrastrukturę krytyczną, zwłaszcza na dostawców usług telekomunikacyjnych oraz firmy energetyczne. Najczęstszą techniką infiltracji stosowaną w cyberwojnie jest phishing, przy czym obie strony stosują ukierunkowane kampanie phishingowe, często z towarzyszącymi im exploitami plikowymi lub innymi szkodliwymi ładunkami, wskazują eksperci. Exploit[43] to kod programu służący do przeprowadzenia ataku wykorzystujący luki w zabezpieczeniach powszechnie wykorzystywanych aplikacji. Phishing jest popularny w cyberwojnie, ponieważ jest prosty, mało ryzykowny, skuteczny i wszechstronny.

Podsumowanie

Jednym z największych zagrożeń cywilizacyjnych XXI wieku jest terroryzm, który wywołuje psychozę strachu i zaniepokojenie mieszkańców całego globu. Obecnie, ochrona cyberprzestrzeni stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa i obronności państwa. Cyberprzestrzeń staje się nową przestrzenią funkcjonowania ludzi, państwa i świata, które przyjmuje postać społeczeństwa sieciowego. Społeczeństwo sieciowe porusza się w organizacji sieciowej, która złożona jest z setek tysięcy połączonych ze sobą sieci komputerów, routerów, przełączników i linii światłowodów, które pozwalają funkcjonować obiektom infrastruktury krytycznej. Cyberterroryzm staje się najbardziej nieprzewidywalnym sposobem oddziaływania zorganizowanych grup na funkcjonowanie i stabilność struktur państwowych. Pojawiła się kategoria infrastruktury krytycznej, której zniszczenie lub uszkodzenie może osłabić zdolność obronną oraz bezpieczeństwo państwa. Główne jej elementy to: telekomunikacja, system energetyczny, system bankowy, produkcja oraz sieć transportu gazu ziemnego i ropy naftowej, transport, system zaopatrzenia w wodę, służby ratownicze oraz ciągłość funkcjonowania administracji publicznej.

Działalność organizacji terrorystycznych w cyberprzestrzeni jest faktem. Organizacje dysponują zarówno potencjałem finansowym, jak i doskonale przygotowaną kadrą informatyków, którzy są gotowi wykorzystać swoje umiejętności realizując cele ideologiczne, ekonomiczne lub polityczne.

[43] J. Kuck, *Bezpieczeństwo informacyjne. Cyberterroryzm*…, op. cit., s.79.

Walka z cyberterroryzmem jest bardzo droga i trudna, ze względu na bezmiar cyberprzestrzeni i ogromne trudności związane ze zlokalizowaniem cyberterrorystów. Walką z cyberterroryzmem zajmują się agendy ONZ m.in. Komitet ds. Zwalczania Terroryzmu oraz NATO w zakresie wojny hybrydowej. Walkę z tego rodzaju zagrożeniami prowadzą również specjaliści z Europol i Interpol. Europol m.in. koordynuje transgraniczne policyjne akcje przeciwko cybergangom, a Interpol wspiera mundurowych walczących z cyberterroryzmem w skali globalnej.

Literatura

1. Cegiełka R., *Zagrożenie terroryzmem. Poczucie bezpieczeństwa na początku XXI wieku oraz wpływ terroryzmu na procesy gospodarcze w wymiarach mikro i makro,* Wydawnictwo Agencja Wydawnicza Synergy Elżbieta Meissner, Warszawa 2015.
2. Dróżdż D., *Terroryzm we współczesnym świecie w świetle prawa. Terror oraz terroryzm międzynarodowy i globalny z prawnego punktu widzenia*. Tom 2, Wydawnictwo My Book, Warszawa 2021.
3. Gałecki A., *Bezpieczeństwo informacji w dobie cyberprzestrzennych zagrożeń,* Wydawnictwo Wyższa Szkoła bezpieczeństwa, Poznań 2021.
4. Górka M., *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa 2014.
5. Kuck J., *Bezpieczeństwo informacyjne. Cyberterroryzm. Przestępczość komputerowa*, Wydawnictwo Państwowej Akademii Nauk Stosowanych w Jarosławiu, Jarosław 2023.
6. Kuźniar R., Bezpieczeństwo międzynarodowe, Wydanie drugie rozszerzone, Wydawnicto naukowe SCHOLAR, Warszawa 2022.
7. Lebiedź J., Krztoń W., Stefaniuk B., *Współczesne wyzwania bezpieczeństwa narodowego. Zarządzanie kryzysowe. Wojna w cyberprzestrzeni. Rzeczywistość wirtualna,* Wydawnictwo Texter, Warszawa 2018.
8. Olech A., *Walka z terroryzmem polskie a francuskie doświadczenie*, Wydawnictwo Difin, Warszawa 2021.
9. Malewska A. Filary-Szczepanik M., *Globalizacja i współzależność*, Wydawnictwo Naukowe Akademii Ignatianum w Krakowie, Kraków 2022.
10. Marczyk M., Stolarz M., Terebiński B., *Bezpieczeństwo działań w cyberprzestrzeni. Wybrane aspekty. Tom I Działania w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2022.
11. Marczyk M., Stolarz M., Terebiński B., *Bezpieczeństwo działań w cyberprzestrzeni. Wybrane aspekty. Tom II Działania w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2022.
12. Różański P., Warmiński A., Chałupczak H*., Zagrożenia bezpieczeństwa i porządku publicznego we współczesnej Polsce (wybrane aspekty),* Akademia Wychowania Fizycznego Józefa Piłsudskiego w Warszawie, Wydział Wychowania Fizycznego i zdrowia w Białej Podlaskiej, Biała Podlaska 2023.

13. Rytko-Marczewska M., *Haktywizm (Cyberterroryzm, Haking, Protest obywatelski, Cyberaktywizm, E- Moblilizacja)* , Wydawnictwo UMCS Lublin, Lublin 2014.
14. Stelmach J., *Bezpieczeństwo terrorystyczne obiektów użyteczności publicznej*, Tom III, Wydawnictwo Difin, Warszawa 2022.
15. Stelmach J., *Bezpieczeństwo terrorystyczne obiektów użyteczności publicznej*, Tom IV, Wydawnictwo Difin, Warszawa 2022.
16. Stelmach J., *Zamachy terrorystyczne. Istota i koncepcja reagowania*, Wydawnictwo Difin, Warszawa 2023.
17. Wojciechowska – Filipek S., Ciekanowski Z., Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki- organizacji- państwa, Wydawnictwo CedeWu, Warszawa 2016.
18. Wojciechowski S., Osiewicz P., *Zrozumieć współczesny terroryzm*, Wydawnictwo Difin, Warszawa 2017.
19. Zieliński T., Mróz P., Bartnik R., *Bezpieczeństwo i obrona Unii Europejskiej*, Akademia Sztuki Wojennej, Warszawa 2020.

Akt prawny

1. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. 1997 Nr 88, poz. 553).

Netografia

1. *Globalizacja – szanse i zagrożenia*, https://globalna.ceo.org.pl/materialy/globalizacja-szanse-i-zagrozenia/.
2. *Globalny*, Słownik PWN, https://sjp.pwn.pl/slowniki/globalny.html.
3. *Infrastruktura krytyczna na celowniku hakerów – czy można ją skutecznie zabezpieczyć?* 12.02.2025, https://academy.asseco.pl/learning-center/infrastruktura-krytyczna-na-celowniku-hakerow-czy-mozna-ja-skutecznie-zabezpieczyc/.
4. Marszycki M., *Cyberwojna między Rosją a Ukrainą wciąż trwa*, 3 marca 2023 r., https://itwiz.pl/cyberwojna-miedzy-rosja-a-ukraina-wciaz-trwa/.
5. Oleksiewicz I., *Cyberterroryzm jako realne zagrożenie dla Polski*, https://rocznikbezpieczenstwa.pl/ojs/index.php/rbm/article/view/449/404.https://rocznikbezpieczenstwa.pl/ojs/index.php/rbm/article/view/449/404.
6. Panas R., *Wojna cybernetyczna i cyberterroryzm – czym są? Czy Polsce grozi cyberwojna?* 10 marca 2022 r., https://nano.komputronik.pl/n/cyberwojna-cyberterroryzm-wojna-cybernetyczna/.
7. Stańczyk M., Lechowicz-Dyl K., *Cyberatak na Lotnicze Pogotowie Ratunkowe. Hakerzy zażądali 390 tys. dolarów okupu*, PAP, 21 lutego 2022 r., https://www.pap.pl/aktualnosci/news%2C1086018%2Ccyberatak-na-lotnicze-pogotowie-ratunkowe-hakerzy-zazadali-390-tys-dolarow.
8. Smolski W., *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*. https://www.repozytorium.uni.wroc.pl/dlibra/publication/67850, [dostęp: 29.03.2025].

dr inż. Marta Chodyka
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0002-8819-2451
https://doi.org/10.29316/9788368103199_7

BEZPIECZEŃSTWO BAZ DANYCH JAKO ELEMENT ODPORNOŚCI CYBERNETYCZNEJ SIŁ ZBROJNYCH

DATABASE SECURITY AS AN ELEMENT OF THE CYBER RESILIENCE OF ARMED FORCES

Streszczenie

Celem rozdziału jest zbadanie roli ochrony baz danych w zapewnieniu cyberodporności sił zbrojnych. Główny problem badawczy sformułowano następująco: jak zabezpieczenie wojskowych baz danych wpływa na tę odporność? Postawiono hipotezę, że wdrożenie skutecznych mechanizmów ochrony (technicznych i organizacyjnych) istotnie wzmacnia cyberodporność sił zbrojnych. Zastosowaną metodą badawczą była jakościowa analiza literatury naukowej oraz dokumentów strategicznych dotyczących bezpieczeństwa narodowego i cyberobrony, ze szczególnym uwzględnieniem środowiska wojskowego. Analiza objęła rolę baz danych, główne cyberzagrożenia oraz kluczowe środki ochrony. Wyniki potwierdzają hipotezę – bezpieczeństwo baz danych stanowi kluczowy filar cyberodporności. Wnioski wskazują na potrzebę integracji ochrony baz danych z wojskową strategią cyberbezpieczeństwa poprzez

Summary

The aim of this chapter is to examine the role of database protection in ensuring the cyber resilience of armed forces. The main research question is: how does securing military databases influence cyber resilience? The hypothesis assumes that implementing effective technical and organizational protection mechanisms significantly strengthens the cyber resilience of armed forces. The adopted research method was a qualitative analysis of scholarly literature and strategic documents concerning national security and cyber defense, with particular emphasis on the military environment. The analysis covered the role of databases, major cyber threats, and key protection measures. The findings confirm the hypothesis – database security constitutes a fundamental pillar of cyber resilience. The conclusions emphasize the need to integrate database protection into the broader military cybersecurity strategy through the

ustanowienie wysokich standardów zabezpieczeń, ciągłe monitorowanie, szkolenie personelu i współpracę z partnerami.

Słowa kluczowe: bezpieczeństwo baz danych, cyberodporność, infrastruktura krytyczna, siły zbrojne, wielowarstwowa obrona, zagrożenia cybernetyczne

establishment of high protection standards, continuous monitoring, personnel training, and cooperation with allied partners.

Keywords: database security, cyber resilience, critical infrastructure, armed forces, defense-in-depth, cyber threats

Wstęp

Współczesne siły zbrojne funkcjonują w silnie zinformatyzowanym środowisku, w którym dane stanowią krytyczny zasób warunkujący powodzenie działań militarnych. Zapewnienie odporności cybernetycznej (cyberodporności) – rozumianej jako zdolność do przygotowania się na zakłócenia, przetrwania ataku oraz szybkiego przywrócenia sprawności systemów po incydencie – stało się jednym z kluczowych wymogów bezpieczeństwa narodowego[1]. W domenie militarnej cyberodporność przekłada się na zdolność sił zbrojnych do utrzymania ciągłości dowodzenia, łączności i realizacji zadań operacyjnych nawet w obliczu agresji w cyberprzestrzeni[2]. Organizacja Traktatu Północnoatlantyckiego NATO (ang. *North Atlantic Treaty Organization*) od kilku lat podkreśla, że odporność – zarówno na poziomie poszczególnych państw, jak i całego Sojuszu – jest warunkiem wiarygodnego odstraszania i efektywnej obrony kolektywnej[3]. Już w 2016 roku NATO wskazała odporność jako fundamentalny element strategii obronnej, określając ją mianem „*pierwszej linii obrony i odstraszania*". W tym kontekście wydano zalecenia dla państw członkowskich, nakładające obowiązek wzmacniania zdolności w zakresie zapewnienia ciągłości działania infrastruktury krytycznej oraz systemów dowodzenia. Zgodnie z art. 3 Traktatu Północnoatlantyckiego[4], każdy członek Sojuszu jest zobowiązany do rozwijania indywidualnych zdolności obronnych, co w praktyce przekłada się na konieczność podejmowania działań

[1] *Resilience as the first line of defence and deterrence*, NATO official publications, 2021.

[2] M. M. Marczyk, M. Stolarz, B. Terebiński (red.), *Cyberbezpieczeństwo: zagrożenia i wyzwania,* Mobilne sieci i systemy teleinformatyczne w cyberbezpieczeństwie Sił Zbrojnych RP, Wydawnictwo Akademii Sztuki Wojennej, Warszawa, 2023, s. 116-157.

[3] *Resilience as the first …*, op. cit.

[4] Umowa między Stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych z 18.06.1964, (Dz. U. 2001.143.1594).

ukierunkowanych na ochronę kluczowych zasobów przed nowymi, często asymetrycznymi, zagrożeniami w cyberprzestrzeni[5].

Siły Zbrojne Rzeczypospolitej Polskiej, podobnie jak armie innych państw NATO, intensywnie rozwijają zdolności cyberobrony. Utworzenie wyspecjalizowanych Wojsk Obrony Cyberprzestrzeni oraz przypisanie wojsku ustawowego zadania „*ochrony i obrony cyberprzestrzeni*" państwa[6] świadczy o rosnącym znaczeniu domeny cyfrowej w systemie obronnym. Doświadczenia ostatnich dwóch dekad unaoczniły, że wojsko musi być przygotowane na zakłócenia w cyberprzestrzeni o charakterze zarówno technicznym, jak i informacyjnym[7]. Utrata dostępu do kluczowych systemów informatycznych lub kompromitacja poufnych danych może sparaliżować dowodzenie i logistykę, zagrażając bezpieczeństwu państwa. Dane od zawsze były decydującym czynnikiem na polu walki, a wyciek informacji może stanowić dla wroga ogromny sukces wywiadowczy. Właśnie dlatego bezpieczeństwo informacji – w szczególności bezpieczeństwo baz danych, które gromadzą i udostępniają te informacje – stało się integralną częścią strategii cyberbezpieczeństwa sił zbrojnych[8].

Celem niniejszego rozdziału jest określenie roli bezpieczeństwa baz danych jako kluczowego elementu budującego odporność cybernetyczną sił zbrojnych. Przedmiotem analizy jest ustalenie, w jakim zakresie oraz w jaki sposób skuteczne zabezpieczenie wojskowych baz danych wpływa na zdolność sił zbrojnych do kontynuowania operacji w warunkach zakłóceń cybernetycznych. W związku z powyższym sformułowano problem badawczy w postaci pytania: w jaki sposób skuteczne zabezpieczenie baz danych w systemach wojskowych wpływa na odporność cybernetyczną sił zbrojnych? Przyjęta hipoteza badawcza zakłada, że odpowiednie zabezpieczenie baz danych – poprzez wdrożenie adekwatnych mechanizmów technicznych oraz procedur organizacyjnych – znacząco wzmacnia odporność cybernetyczną sił zbrojnych, chroniąc kluczowe informacje przed utratą lub ingerencją oraz zapewniając ciągłość operacyjną nawet w sytuacji wystąpienia cyberataku. Innymi

[5] J. Keplin, *Budowanie odporności państwa na działania hybrydowe*, Przegląd Bezpieczeństwa Wewnętrznego, Numer 29(15), 2023, s. 13-38.

[6] B. Kuś, *Siły Zbrojne Rzeczypospolitej Polskiej a cyberbezpieczeństwo. Zagadnienia organizacyjno-prawne*, Cybersecurity & Law, nr 2, 2023, s. 32-50.

[7] M. Pollard, *A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States*, Pepperdine Policy Review: Vol. 16, Article 1, 2024.

[8] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, Warszawa 2019.

słowy, im wyższy poziom bezpieczeństwa baz danych, tym wyższa ogólna cyberodporność struktur wojskowych. W celu weryfikacji powyższej hipotezy w rozdziale przeanalizowano istniejące koncepcje odporności w cyberprzestrzeni w kontekście bezpieczeństwa narodowego, określono znaczenie baz danych dla funkcjonowania systemów wojskowych, zidentyfikowano główne zagrożenia skierowane przeciwko wojskowym bazom danych oraz dokonano oceny skuteczności wybranych środków ochrony w kontekście utrzymania ciągłości działania systemów militarnych. Dla pogłębienia analizy sformułowano także pytania pomocnicze, w tym: jakie wyzwania w zakresie bezpieczeństwa informacji wynikają ze współczesnych strategii i doktryn obronnych, jakie rodzaje ataków stanowią największe zagrożenie dla baz danych sił zbrojnych oraz które metody zabezpieczeń mają największe znaczenie z perspektywy odporności systemów wojskowych. Niniejsze opracowanie ma charakter jakościowy i koncepcyjny. Zastosowano metodę analizy treści dostępnej literatury naukowej oraz dokumentów strategicznych dotyczących bezpieczeństwa informacji i obronności. Szczególną uwagę poświęcono krajowym dokumentom takim jak, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 oraz Resortowa strategia sztucznej inteligencji do roku 2039, a także doktrynom NATO i wytycznym instytucji międzynarodowych zajmujących się cyberbezpieczeństwem, m.in. ENISA (ang. *European Union Agency for Cybersecurity*) oraz NATO CCDCOE (ang. *Cooperative Cyber Defence Centre of Excellence*). Celem przyjętej metodologii było wyodrębnienie kluczowych ram pojęciowych i teoretycznych oraz identyfikacja powtarzających się zagrożeń i postulatów dotyczących ochrony baz danych w środowisku wojskowym. Analizie poddano także wybrane przypadki incydentów cybernetycznych opisywane w dostępnej literaturze przedmiotu, które posłużyły jako ilustracja praktycznych konsekwencji niewystarczającego zabezpieczenia danych operacyjnych. Ze względu na analityczno-koncepcyjny charakter pracy wnioski sformułowano na podstawie syntezy danych wtórnych – konfrontacji ustaleń literaturowych z aktualnym kontekstem strategicznym i organizacyjnym sił zbrojnych. Takie podejście umożliwiło sformułowanie wniosków o charakterze ogólnym, odnoszących się do systemowego znaczenia bezpieczeństwa baz danych w zapewnieniu cyberodporności struktur wojskowych. Analizę prowadzono z uwzględnieniem trzech poziomów: strategicznego (strategie i doktryny bezpieczeństwa), organizacyjnego (struktury i procedury instytucji wojskowych) oraz technicznego (mechanizmy zabezpieczające i architektura systemów informacyjnych).

Odporność systemów informacyjnych

Pojęcie odporności (ang. *resilience*) w kontekście bezpieczeństwa narodowego i wojskowego zyskało na znaczeniu w ostatnich latach, znajdując odzwierciedlenie w strategiach państwowych oraz analizach akademickich. Odporność cybernetyczna najczęściej definiowana jest jako zdolność systemu lub organizacji do przygotowania się na incydenty, przetrwania ataku oraz odzyskania zdolności działania w możliwie najkrótszym czasie[9]. NATO w oficjalnych dokumentach opisuje odporność jako umiejętność „*przygotowania się, wytrwania, reagowania oraz szybkiego odzyskania sprawności po strategicznych wstrząsach i zakłóceniach*" [10]. Ujęcie to podkreśla, że odporność jest procesem wieloetapowym, obejmującym zarówno fazę prewencji (przygotowania i wzmocnienia systemów), fazę reakcji w trakcie zagrożenia, jak i fazę odbudowy po incydencie.

W literaturze przedmiotu wskazuje się, że odporność stanowi kluczowy element nowoczesnej koncepcji odstraszania i obrony[11]. Rozumiana jako gotowość państwa, sprawność organizacyjna oraz przygotowanie infrastruktury krytycznej, stanowi fundament skutecznej reakcji na działania poniżej progu wojny – w tym zagrożenia cybernetyczne i dezinformację. Analizy NATO oraz niezależnych ośrodków badawczych potwierdzają, że odporność cybernetyczna systemów dowodzenia i łączności wymaga wdrażania strategii wielowarstwowej obrony oraz redundancji, które pozwolą na utrzymanie funkcji operacyjnych mimo zakłóceń[12]. Odporność nie polega na całkowitej niewrażliwości systemu, lecz na zdolności ograniczania skutków ataku i szybkiego odzyskania sprawności działania[13].

W kontekście sił zbrojnych szczególne znaczenie przypisuje się ciągłości działania systemów dowodzenia, łączności oraz ochronie danych operacyjnych. Koncepcja *mission assurance* zakłada konieczność zabezpieczenia

[9] M. P. Sallos, A. Garcia Perez, A. Bocanet, *Organisational cyber resilience: a heuristic for bridging foundations and applications*, Journal of Enterprise Information Management, 37(6), 2024, s. 1926-1952.

[10] *Resilience as the first …*, op. cit.

[11] J. P. Yaacoub, H. Noura, O. Salman, A, Chehab, *Security analysis of drones systems: Attacks, limitations, and recommendations*, Internet of Things, 11, 100218, 2020.

[12] A. Afina, R. Inverarity, B. Unal, *Cyber Resilience in NATO Command and Control Systems*. London: Chatham House, 2020.

[13] *Allied Command Transformation (ACT)*, Cyber Resilience Strategic Concept. Norfolk, VA, 2023.

wszystkich krytycznych komponentów infrastruktury wojskowej – w tym baz danych – przed różnymi typami zagrożeń. W literaturze krajowej zwraca się uwagę, że cyberbezpieczeństwo państwa obejmuje nie tylko ochronę systemów teleinformatycznych, ale także danych w nich przetwarzanych – co jednoznacznie wiąże ochronę baz danych z cyberodpornością narodową[14]. Równocześnie postuluje się dostosowanie systemu prawnego oraz struktur organizacyjnych sił zbrojnych do nowych wyzwań w domenie cyber[15].

Od strony technicznej, bezpieczeństwo baz danych było analizowane od dawna w kontekście informatyki i kryptografii, jednak dopiero niedawno pojawiły się badania poświęcone ich roli w środowisku militarnym[16]. Kluczowe cele bezpieczeństwa danych określane są w literaturze jako triada CIA – *Confidentiality*, *Integrity*, *Availability* – a w kontekście wojskowym poszerza się je o autentyczność i niezaprzeczalność informacji[17]. Przegląd aktualnych raportów pokazuje, że ataki ukierunkowane na wojskowe systemy informacyjne, w tym bazy danych, mogą skutkować naruszeniem każdego z tych atrybutów, zagrażając poufności danych operacyjnych, integralności komunikacji oraz dostępności zasobów w czasie rzeczywistym. W odpowiedzi na te wyzwania, zarówno w Stanach Zjednoczonych, jak i w Polsce, rozpoczęto działania mające na celu określenie strategii rozwoju sztucznej inteligencji w środowisku militarnym, w tym w kontekście ochrony danych. Raport GAO[18] szczegółowo analizuje stan rozwoju zdolności związanych z AI w systemach uzbrojenia, zwracając uwagę na potrzebę zapewnienia niezawodności i bezpieczeństwa komponentów informacyjnych, takich jak bazy danych. Z kolei polska „*Resortowa strategia sztucznej inteligencji do roku 2039"* opracowana przez MON[19] wskazuje kierunki rozwoju sztucznej inteligencji w Siłach Zbrojnych RP,

[14] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, Warszawa 2019.

[15] W. Kitler, K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska, *System bezpieczeństwa w cyberprzestrzeni RP*, Towarzystwo Wiedzy Obronnej, Warszawa 2018.

[16] H. Ahmad, I. Dharmadasa, F. Ullah, M. A. Babar, *A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures*, arXiv preprint arXiv:2104.11906, 2021 oraz A. Singh, *Military Computing Security: Insights and Implications*, Journal of Institution of Engineers (India): Series B, 104(3), 2023, s. 359-366.

[17] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2024.

[18] *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon System*s, GAO-24-106221, Washington, DC: U.S. Government Accountability Office, 2024.

[19] *Resortowa strategia sztucznej inteligencji do roku 2039*, Ministerstwo Obrony Narodowej, Warszawa, 2020.

uwzględniając ochronę infrastruktury informacyjnej jako elementu cyberodporności systemów obronnych.

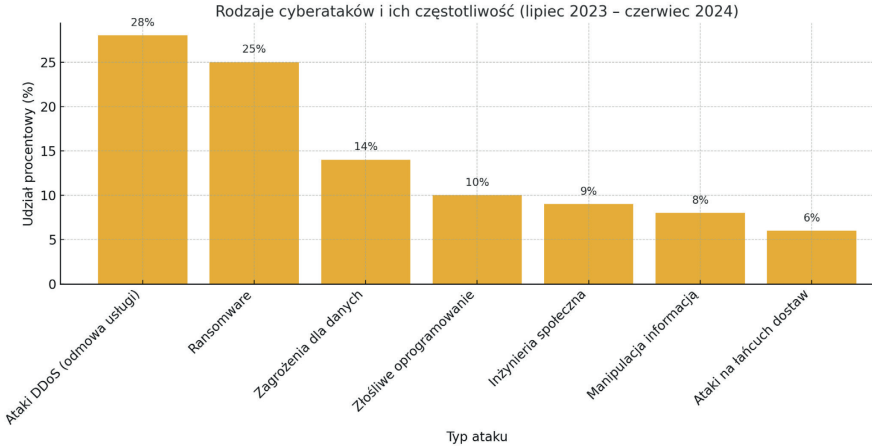
Podsumowując, dotychczasowe badania oraz dokumenty strategiczne jednoznacznie wskazują, że cyberodporność jest warunkiem sprawnego działania struktur państwowych i wojskowych w środowisku pełnym dynamicznych zagrożeń, a ochrona baz danych jako elementu krytycznej infrastruktury informacyjnej powinna stanowić jeden z priorytetów systemów bezpieczeństwa narodowego. Ujęcie to znajduje odzwierciedlenie zarówno w analizach międzynarodowych, takich jak raport GAO, jak i w krajowych dokumentach strategicznych, które wskazują na konieczność kompleksowego podejścia do bezpieczeństwa danych w środowisku operacyjnym oraz uwzględnienia specyfiki wojskowych systemów informacyjnych przy projektowaniu mechanizmów ochronnych.

Znaczenie baz danych w systemach wojskowych

Bazy danych stanowią strategiczny komponent systemów informacyjnych współczesnych sił zbrojnych, odgrywając zasadniczą rolę w planowaniu, prowadzeniu oraz zabezpieczaniu operacji militarnych. Ich znaczenie wynika nie tylko z funkcji przechowywania i przetwarzania informacji, lecz także z roli, jaką odgrywają w zapewnianiu ciągłości dowodzenia i wsparcia decyzyjnego w warunkach konfliktu zbrojnego. Bazy te obejmują zbiory danych personalnych, operacyjnych, logistycznych, technicznych, a także dane związane z rozpoznaniem i analizą zagrożeń.

W dobie rosnącej cyfryzacji sfery militarnej systemy bazodanowe stają się celem ataków ze strony zorganizowanych podmiotów – w tym grup przestępczych, cyberaktywistów oraz tzw. trwałych zagrożeń zaawansowanych (ang. *Advanced Persistent Threats*, APT)[20], często powiązanych z interesami państwowymi. Dane przedstawione w *ENISA Threat Landscape 2024* wskazują, że w okresie od lipca 2023 do czerwca 2024 zagrożenia dla dostępności systemów, *ransomware* oraz ataki na dane stanowiły trzy najczęściej odnotowywane formy ataków cybernetycznych. Łącznie odpowiadały one za ponad połowę wszystkich incydentów. Zestawienie tych danych prezentuje rysunek 1, który ilustruje udział procentowy poszczególnych typów ataków w globalnym krajobrazie zagrożeń.

[20] T. Wrightson, *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization,* McGraw Hill, 2024.



Rysunek 1. Rodzaje cyberataków i ich częstotliwość (lipiec 2023 – czerwiec 2024)
Źródło: opracowanie własne na podstawie: European Union Agency for Cybersecurity (ENISA)[21].

Co istotne, ataki typu DDoS (ang. *Distributed Denial of Service*) po raz pierwszy wyprzedziły *ransomware* pod względem liczby przypadków, wskazując na zmianę dominujących strategii przeciwników. Znaczący udział ataków ukierunkowanych na systemy bazodanowe potwierdza konieczność traktowania ochrony danych jako jednego z priorytetów strategicznych w ramach bezpieczeństwa informacyjnego sił zbrojnych. Bazy danych stały się nie tylko celem ataków szyfrujących (np. *ransomware*), ale również areną operacji dezinformacyjnych, kradzieży informacji (*infostealerów*), sabotażu integralności danych oraz działań wykorzystujących techniki ukrywania się w infrastrukturze chmurowej i kanałach komunikacyjnych (np. *Slack, Telegram*). Warto także odnotować rosnącą rolę manipulacji informacjami z użyciem sztucznej inteligencji oraz wykorzystywanie inżynierii społecznej do kompromitacji zaufanych projektów *open source*. Oznacza to, że zagrożenia wobec baz danych nie ograniczają się jedynie do aspektów technicznych, ale obejmują również wymiar socjotechniczny i geopolityczny. Zróżnicowanie metod ataku wymusza stosowanie kompleksowych i wielowarstwowych mechanizmów zabezpieczeń, obejmujących zarówno szyfrowanie i segmentację dostępu, jak i monitoring aktywności, testowanie podatności, audyty oraz szkolenia personelu. Tylko zintegrowane podejście może zapewnić odpowiedni poziom cyberodporności struktur wojskowych wobec zmieniającego się krajobrazu zagrożeń.

[21] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024*, 2024.

Współczesne zagrożenia wobec wojskowych baz danych przybierają charakter wielowymiarowy i coraz częściej wpisują się w szerszy kontekst kampanii hybrydowych prowadzonych przez aktorów państwowych oraz zorganizowane grupy cyberprzestępcze. Analiza danych zawartych w raporcie *ENISA Threat Landscape* 2024[22] pozwala na identyfikację dominujących trendów w zakresie ataków wymierzonych w strategiczne zasoby informacyjne, w tym w szczególności w systemy bazodanowe, pełniące kluczową rolę w infrastrukturze dowodzenia, rozpoznania, logistyki i analizy operacyjnej sił zbrojnych.

Jednym z fundamentalnych typów zagrożeń pozostają ataki aplikacyjne, w tym przede wszystkim wstrzykiwanie zapytań w języku strukturalnym (*SQL Injection*), które umożliwiają nieautoryzowany dostęp do danych, ich modyfikację lub trwałe usunięcie. Mechanizm tego rodzaju ataku polega na wprowadzeniu do aplikacji danych wejściowych w taki sposób, aby zostały one przetworzone jako część instrukcji SQL, co prowadzi do wykonania niezamierzonych operacji w bazie danych. W kontekście wojskowym, skuteczny atak typu *SQL Injection* może doprowadzić do kompromitacji informacji niejawnych, ujawnienia parametrów uzbrojenia lub lokalizacji jednostek operacyjnych, co stanowi poważne zagrożenie dla bezpieczeństwa narodowego[23]. Równolegle obserwuje się wzrost liczby incydentów wykorzystujących podatności typu zero-day oraz techniki ataków na komponenty pośredniczące, takie jak biblioteki mapowania obiektowo-relacyjnego czy *frameworki* interfejsów API. Tego rodzaju luki, zanim zostaną zidentyfikowane i załatane przez producentów, stają się wektorem wejściowym dla ataków ukierunkowanych, często inicjowanych przez wyspecjalizowane grupy APT (ang. *Advanced Persistent Threats*). Szczególnie niebezpieczne są ataki wykorzystujące połączenie podatności i socjotechniki, które umożliwiają trwałą infiltrację systemów oraz eskalację uprawnień w infrastrukturze wojskowe[24]. Kolejną kategorią zagrożeń są incydenty z wykorzystaniem złośliwego oprogramowania, zwłaszcza typu *ransomware* i tzw. *wipery* (ang. *data-wiping malware*). *Ransomware* prowadzi do zaszyfrowania zasobów informacyjnych i wymuszenia okupu za ich odszyfrowanie, co może sparaliżować operacje wojskowe poprzez utratę dostępu do danych rozpoznawczych, planistycznych czy logistycznych. *Wipery* natomiast – podszywające się pod *ransomware* – realizują trwałe uszkodzenie danych,

[22] European Union Agency for Cybersecurity (ENISA)*, ENISA Threat Landscape 2024*, 2024.

[23] J. Clarke, *SQL Injection Attacks and Defense*, Syngress, 2012.

[24] R. Rais, C. Morillo, E. Gilman, D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Network*, 2nd Edition, Helion, Gliwice 2024.

często w sposób nieodwracalny, służąc jako narzędzie sabotażu informacyjnego w ramach działań kinetycznych i niekinetycznych. Oprogramowanie tego typu coraz częściej wykorzystuje techniki *Living Off the Land* (LOTL) i *Living Off Trusted Sites* (LOTS), operując w ramach zaufanych usług chmurowych lub kanałów komunikacyjnych (np. *Slack, Telegram*), co znacząco utrudnia jego detekcję i eliminację[25]. Niemniej istotnym zagrożeniem są ataki na integralność danych, prowadzone w sposób ukryty i trudny do wykrycia. Przeciwnik, który uzyska dostęp do systemu, może dokonać subtelnej modyfikacji danych operacyjnych, technicznych lub rozpoznawczych – np. zmieniając współrzędne celów, charakterystyki uzbrojenia lub parametry logistyczne. Efektem takich działań może być błędne decyzje dowódcze podejmowane na podstawie zmanipulowanej informacji. Skuteczna ochrona integralności wymaga wdrożenia polityki audytów, systemów wykrywania anomalii oraz stosowania mechanizmów spójności danych i zasady ograniczonego dostępu (ang. *least privilege*). Zagrożenia wewnętrzne (ang. *insider threats*), czyli działania podejmowane przez osoby posiadające autoryzowany dostęp do infrastruktury, stanowią kolejny istotny wektor ataku. Tego rodzaju incydenty są trudne do wykrycia ze względu na legalność dostępu oraz często brak jednoznacznych wskaźników naruszenia. Pomimo ich niskiej reprezentacji w statystykach, potencjalne skutki takich działań są katastrofalne, szczególnie gdy dotyczą systemów dowodzenia i kontroli. W ujęciu strategicznym, wojskowe bazy danych stają się celem kampanii prowadzonych przez grupy powiązane z wywiadem obcych państw, realizujących długotrwałą infiltrację środowisk informacyjnych. Działania te charakteryzują się wysokim stopniem ukrycia, wykorzystaniem szyfrowanej komunikacji, tunelowaniem danych oraz przechwytywaniem informacji poprzez kanały nieobjęte monitoringiem. Tego typu operacje są często trudne do wykrycia bez zastosowania zaawansowanych narzędzi klasy SIEM, DAM czy UEBA. W odpowiedzi na ewoluujące zagrożenia, raport ENISA rekomenduje wdrażanie modelu obrony warstwowej (ang. *defense-in-depth*), który uwzględnia nie tylko zabezpieczenia techniczne i kryptograficzne, ale również aspekty organizacyjne, szkoleniowe oraz proceduralne. Szczególny nacisk położony jest na rozwój odporności poprzez segmentację sieci, monitorowanie aktywności użytkowników, regularne audyty, szyfrowanie danych, a także testowanie odporności systemów na złożone scenariusze ataków – zarówno symulowane, jak i rzeczywiste.

[25] M. Sikorski, A. Honig, *Praktyczna Analiza Malware*. Przewodnik po usuwaniu złośliwego oprogramowania, Wydawnictwo Naukowe PWN, Warszawa 2021.

Współczesne ataki na wojskowe systemy informacyjne często przybierają postać złożonych kampanii, realizowanych zgodnie z koncepcją łańcucha ataku (ang. *kill chain*)[26]. Tego rodzaju działania są szczególnie charakterystyczne dla trwałych zagrożeń zaawansowanych (APT), które w sposób systematyczny prowadzą kampanie cyberszpiegowskie przeciwko instytucjom wojskowym. Podział ataku na poszczególne fazy pozwala na lepsze zrozumienie jego struktury i identyfikację potencjalnych punktów przeciwdziałania. Etapy złożonego ataku na bazę danych przedstawiona została w tabeli 1.

Tabela 1. Etapy złożonego ataku na bazę danych (model łańcucha ataku)

Faza	Opis działań
1. Rekonesans	Identyfikacja celu ataku (np. administratora systemu) oraz zebranie informacji przy użyciu metod z ogólnodostępnych źródeł (ang. *Open Source Intelligence*, OSINT).
2. Przekazanie	Dostarczenie złośliwego kodu, zwykle za pomocą ataku ukierunkowanego typu *spear phishing*.
3. Wykorzystanie	Uruchomienie podatności w oprogramowaniu (np. *exploit* przeglądarki lub klienta bazy danych).
4. Instalacja	Implementacja złośliwego oprogramowania (np. trojan zdalnego dostępu ang. Remote Access Trojan, RAT) na stacji roboczej ofiary.
5. Komunikacja (C2)	Nawiązanie kanału dowodzenia (ang. *Command and Control*, C2) i sterowanie zainfekowanym systemem.
6. Eskalacja	Uzyskanie wyższych uprawnień, ruch lateralny w sieci, przejęcie dodatkowych urządzeń i serwerów.
7. Działania końcowe	Eksfiltracja danych lub ich sabotaż (np. modyfikacja, usunięcie, zaszyfrowanie).

Źródło: opracowanie własne.

Każdy z wymienionych etapów może wykorzystywać odmienne techniki ataku i wymaga odmiennych mechanizmów detekcji oraz reakcji. Dla przykładu, faza rekonesansu może być ograniczona przez zastosowanie polityki ograniczonego ujawniania struktur organizacyjnych, faza dostarczenia – przez filtrowanie wiadomości i edukację personelu, faza wykorzystania – przez aktualizację i *hardening* systemów, a działania końcowe – przez zastosowanie mechanizmów audytu i monitoringu aktywności w bazie danych. Złożoność tych ataków polega na ich zdolności do ukrywania obecności intruza w systemie przez długi czas. Często wykorzystują one złośliwe oprogramowanie typu bezplikowego (ang. *fileless malware*), techniki tunelowania danych, ukrywanie zapytań w legalnym

[26] J. Dimaggio, *Art Of Cyberwarfare, An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*, No Starch Press,US, 2022.

ruchu sieciowym, a także eksfiltrację poprzez kanały trudne do wykrycia[27]. Konsekwencją tego jest znaczne wydłużenie tzw. czasu wykrycia (ang. *dwell time*), który w środowisku militarnym może oznaczać realne zagrożenie dla bezpieczeństwa państwa. Wnioski płynące z analizy modelu łańcucha ataku pokazują, że skuteczne przeciwdziałanie wymaga nie tylko technologii, lecz także procedur organizacyjnych i odpowiednio przeszkolonego personelu. Tylko podejście wielowarstwowe – obejmujące edukację użytkowników, detekcję zagrożeń, mechanizmy prewencji i strategię reakcji – może zapewnić odporność systemów wojskowych baz danych na współczesne zagrożenia cybernetyczne.

Kluczowe środki ochrony baz danych w kontekście cyberodporności

Zabezpieczenie wojskowych systemów bazodanowych stanowi jeden z kluczowych elementów budowania odporności cybernetycznej sił zbrojnych. Wymaga to wdrożenia kompleksowej architektury ochronnej, która obejmuje mechanizmy techniczne, proceduralne oraz organizacyjne[28]. Poniższe środki zabezpieczające uznaje się za fundamentalne z punktu widzenia odporności informacyjnej systemów militarnych:

1) Kontrola dostępu i zarządzanie tożsamością. Efektywne zarządzanie dostępem do baz danych wymaga bezwzględnego przestrzegania zasady ograniczonego dostępu do informacji (ang. *need-to-know*). Oznacza to konieczność wdrożenia mechanizmów uwierzytelniania wieloskładnikowego (ang. *Multi-Factor Authentication*, MFA) oraz scentralizowanych systemów zarządzania tożsamościami i uprawnieniami (ang. *Identity and Access Management*, IAM). Ponadto, serwery baz danych powinny być umieszczone w wyodrębnionych segmentach sieci (np. strefie buforowej, ang. *Demilitarized Zone*, DMZ), z dostępem jedynie z poziomu zaufanych węzłów administracyjnych (tzw. serwerów pośredniczących, ang. *jump servers*). Obowiązkiem administratorów jest również cykliczna weryfikacja i audyt uprawnień użytkowników, zgodnie z zasadą minimalnego zakresu uprawnień (ang. *least privilege*).
2) Szyfrowanie danych w spoczynku i transmisji. Zastosowanie algorytmów kryptograficznych jest nieodzownym elementem ochrony poufności

[27] M. Serafin, *Bezpieczeństwo sieci firmowej. Kontrola ruchu wychodzącego*, Helion, Gliwice 2022.

[28] M. Kowalewski, Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017.

danych zarówno w stanie spoczynku (ang. *data at rest*), jak i w trakcie transmisji (ang. *data in transit*). Zalecane jest stosowanie szyfrowania na poziomie plików oraz transmisji sieciowej z użyciem protokołów bezpiecznych, takich jak *Transport Layer Security* (TLS). Dla zwiększenia bezpieczeństwa operacyjnego, mechanizmy szyfrowania powinny być zgodne ze standardami zatwierdzonymi dla środowisk o znaczeniu strategicznym (np. FIPS 140-2) i wspierane przez sprzętowe moduły zarządzania kluczami (ang. *Hardware Security Modules*, HSM). Ochronie szyfrowaniem powinny podlegać również kopie zapasowe, przechowywane poza główną infrastrukturą operacyjną.

3) Monitorowanie i detekcja anomalii. Rozbudowane mechanizmy monitorowania są konieczne do identyfikacji prób naruszeń bezpieczeństwa. Systemy klasy *Database Activity Monitoring* (DAM) umożliwiają bieżące śledzenie i analizę operacji wykonywanych na bazach danych, wykrywając m.in. nietypowe zapytania, próby eskalacji uprawnień, czy masowe eksporty danych[29]. Komplementarnie, narzędzia *Security Information and Event Management* (SIEM) oraz struktury *Security Operations Center* (SOC) pozwalają na korelację zdarzeń w skali całej organizacji i skracają czas identyfikacji obecności nieautoryzowanego podmiotu w infrastrukturze (tzw. *dwell time*). W jednostkach wojskowych zaleca się funkcjonowanie zespołów szybkiego reagowania na incydenty (ang. *Computer Security Incident Response Team*, CSIRT), pełniących funkcję ciągłego nadzoru.
4) Redundancja i kopie zapasowe. Zdolność do przywrócenia ciągłości funkcji operacyjnych wymaga prowadzenia regularnej polityki tworzenia kopii zapasowych danych, realizowanej według modelu 3-2-1 (trzy kopie, na dwóch różnych nośnikach, jedna poza główną lokalizacją – *off-site*). Kopie te powinny być izolowane od sieci operacyjnej, co zabezpiecza je przed atakami typu *ransomware*. Ponadto rekomendowane jest wdrożenie architektury wysokiej dostępności, z replikacją danych do centrów zapasowych, przy użyciu mechanizmów automatycznego przełączenia węzła (ang. *failover*). Tego typu redundancja pełni funkcję zarówno technicznej ochrony zasobów, jak i psychologicznego odstraszania przeciwnika, redukując spodziewaną skuteczność ataku.

[29] J. Bandler, A Merzon, *Cybercrime Investigations A Comprehensive Resource for Everyone*, Taylor & Francis Ltd, 2022.

5) Zarządzanie podatnościami i twarda konfiguracja. Zapewnienie zgodności systemu bazodanowego z wymaganiami bezpieczeństwa obejmuje stosowanie procedur aktualizacji (ang. *patch management*) oraz tzw. twardej konfiguracji (ang. *hardening*). Zaleca się okresowe stosowanie list kontrolnych opartych o wytyczne organizacji takich jak Departament Obrony Stanów Zjednoczonych (np. *Security Technical Implementation Guides* – STIG) czy Sojusz Północnoatlantycki (*Baseline Security Requirements*). Praktyki te obejmują m.in. dezaktywację nieużywanych funkcjonalności, filtrowanie portów, rotację kluczy kryptograficznych oraz wdrożenie polityk silnych haseł.
6) Szkolenie i standaryzacja działań personelu. Czynniki ludzkie pozostają jednym z najistotniejszych obszarów ryzyka dla systemów informacyjnych. Stąd kluczowe znaczenie ma systematyczne prowadzenie szkoleń i ćwiczeń z zakresu ochrony danych, w tym symulacji zagrożeń typu *phishing* oraz reagowania na incydenty. Siły zbrojne winny wdrażać instytucjonalne programy podnoszenia świadomości zagrożeń cybernetycznych oraz rozwijać kompetencje administratorów i operatorów systemów. Polityki bezpieczeństwa muszą jasno określać reguły postępowania, obowiązki personelu oraz procedury eskalacji incydentu. Przykładem dobrych praktyk w tym zakresie są ćwiczenia NATO *Locked Shields*, które umożliwiają praktyczne sprawdzenie gotowości struktur obronnych wobec realnych scenariuszy zagrożeń[30]. *Locked Shields* to największe na świecie ćwiczenia typu „live-fire" w zakresie cyberobrony, organizowane przez Centrum Doskonałości NATO ds. Współpracy w Zakresie Cyberobrony, (ang. *Cooperative Cyber Defence Centre of Excellence*, NATO CCDCOE). Uczestnicy – zespoły z różnych państw – muszą chronić systemy teleinformatyczne oraz krytyczną infrastrukturę fikcyjnego państwa przed złożonymi i zsynchronizowanymi atakami przeprowadzanymi przez zespół agresora, co pozwala im doskonalić zarówno umiejętności techniczne, jak i koordynację operacyjną w warunkach zbliżonych do rzeczywistych[31].

Skuteczna ochrona zasobów informacyjnych wymaga jednak nie tylko wdrażania pojedynczych środków zabezpieczających, lecz również ich uporządkowania w ramach kompleksowego, wielowarstwowego modelu obrony. Takie podejście umożliwia zintegrowane zarządzanie ryzykiem oraz zwiększa

[30] NATO CCDCOE, *Locked Shields – The World's Largest and Most Complex International Live-Fire Cyber Defence Exercise,* 2025.

[31] Locked Shields, https://ccdcoe.org/locked-shields/, [dostęp: 02.03.2025].

odporność infrastruktury na złożone, wieloetapowe ataki. Warstwowy model ochrony baz danych w systemie cyberodporności sił zbrojnych przedstawiony został na rysunku 2.



Rysunek 2. Warstwowy model ochrony baz danych w systemie cyberodporności sił zbrojnych
Źródło: opracowanie własne.

Każdy z przedstawionych środków ochronnych pełni określoną funkcję w warstwowym modelu bezpieczeństwa. Ich synergiczne wdrożenie prowadzi do znaczącego zwiększenia odporności organizacyjnej sił zbrojnych na zakłócenia w domenie informacyjnej. Ochrona baz danych jako zasobu o charakterze krytycznym, musi zostać osadzona w szerszym systemie zarządzania bezpieczeństwem informacyjnym, odpowiadającym aktualnym zagrożeniom oraz specyfice środowiska wojskowego.

Podsumowanie

W świetle przeprowadzonych analiz można stwierdzić, że bezpieczeństwo baz danych stanowi fundamentalny element budowania cyberodporności sił zbrojnych. Chroniąc krytyczne informacje i zapewniając ciągłość działania w warunkach cyberzagrożeń, efektywne zabezpieczenie wojskowych baz danych bezpośrednio przekłada się na zdolność armii do przetrwania ataków oraz szybkiego odtworzenia gotowości operacyjnej po incydencie. Wyniki

pracy potwierdziły postawioną hipotezę – wdrożenie skutecznych mechanizmów ochrony baz danych znacząco wzmacnia odporność cybernetyczną organizacji wojskowych. Jednocześnie wykazano, że zagrożenia skierowane przeciwko bazom danych mają charakter wielowymiarowy (od klasycznych ataków aplikacyjnych, poprzez ataki socjotechniczne, aż po zaawansowane, wieloetapowe operacje APT finansowane przez państwa), co oznacza, że nie istnieje jedno rozwiązanie gwarantujące pełne bezpieczeństwo. Wymagana jest kompleksowa, wielowarstwowa strategia obrony, łącząca aspekty techniczne, proceduralne i organizacyjne, aby zminimalizować ryzyko naruszeń na każdym etapie ataku i zapewnić odporność systemów informacyjnych. W trakcie badań zidentyfikowano kluczowe obszary zabezpieczenia wojskowych baz danych, które powinny funkcjonować w sposób komplementarny. Do fundamentalnych środków ochrony należą przede wszystkim: ścisła kontrola dostępu i zarządzanie tożsamością użytkowników (m.in. zasada najmniejszych uprawnień, uwierzytelnianie wieloskładnikowe, segmentacja sieci i odseparowanie serwerów baz danych), szyfrowanie danych w spoczynku i podczas transmisji zgodnie z najwyższymi standardami kryptograficznymi, rozbudowane mechanizmy monitorowania aktywności i detekcji anomalii (np. systemy klasy SIEM/DAM oraz zespoły szybkiego reagowania CSIRT), a także zapewnienie redundancji i regularne tworzenie izolowanych kopii zapasowych. Istotnym elementem jest również ciągłe zarządzanie podatnościami i twarda konfiguracja systemów (regularne aktualizacje, audyty bezpieczeństwa, zgodność ze standardami typu STIG), uzupełniane przez systematyczne szkolenie personelu oraz standaryzację procedur. Synergiczne wdrożenie tych zróżnicowanych środków tworzy warstwowy system ochrony, który skutecznie podnosi odporność całej infrastruktury informacyjnej – nawet jeśli pojedynczy mechanizm zawiedzie, pozostałe elementy mogą zapobiec eskalacji incydentu i utrzymać kluczowe funkcje operacyjne. Uzyskane wyniki mają istotne znaczenie praktyczne dla kształtowania polityki cyberbezpieczeństwa w sektorze obronnym. Przede wszystkim wskazują na potrzebę trwałej integracji ochrony baz danych z szerszą strategią cyberobrony sił zbrojnych. Rekomenduje się, aby bezpieczeństwo danych zostało uwzględnione w doktrynach i planach operacyjnych jako jeden z priorytetów obrony infrastruktury krytycznej. Planowanie i rozwój systemów wojskowych powinny obejmować ustanowienie wysokich standardów zabezpieczeń (zarówno technologicznych, jak i proceduralnych), wdrożenie stałego monitoringu zagrożeń i mechanizmów wczesnego ostrzegania, regularne szkolenia specjalistyczne oraz ćwiczenia symulacyjne,

a także ścisłą współpracę z partnerami (np. w ramach sojuszniczych platform wymiany informacji o incydentach czy ćwiczeń, takich jak Locked Shields). Takie holistyczne podejście zapewni, że ochrona baz danych nie będzie odizolowanym wysiłkiem, lecz częścią zintegrowanego systemu odporności cybernetycznej armii. Ze względu na analityczno-koncepcyjny charakter badań, wnioski mają charakter uogólniony i wskazują kierunki działań, wymagając dalszego pogłębienia w przyszłych pracach. Warto podkreślić, że brak empirycznej weryfikacji stanowi naturalne ograniczenie niniejszego studium – stąd pożądane są dalsze badania ukierunkowane na praktyczne sprawdzenie sformułowanych postulatów. Zasadne byłoby przeprowadzenie pogłębionych analiz przypadków rzeczywistych incydentów skierowanych przeciw bazom danych sił zbrojnych oraz symulacji ataków w kontrolowanych warunkach, aby ilościowo ocenić skuteczność poszczególnych mechanizmów obronnych. Kolejnym kierunkiem badań powinno być dostosowanie proponowanych środków ochrony do rozwijających się technologii – takich jak, sztuczna inteligencja czy komputery kwantowe – oraz do ewoluujących wektorów ataku. Kontynuacja badań nad odpornością cybernetyczną wojskowych baz danych, połączona z wymianą doświadczeń między jednostkami naukowymi a instytucjami obronnymi, przyczyni się do dalszego doskonalenia zdolności ochrony informacji w siłach zbrojnych.

Podsumowując, bezpieczeństwo baz danych to nie tylko kwestia techniczna, ale strategiczny czynnik determinujący zdolność armii do działania w obliczu współczesnych zagrożeń – jego wzmacnianie powinno być stałym elementem rozwoju systemu obronnego państwa.

Literatura

1. Afina, A.,Inverarity, R.,Unal, B., *Cyber Resilience in NATO Command and Control Systems*. London: Chatham House, 2020.
2. Ahmad, H., Dharmadasa, I., Ullah, F., Babar, M. A., *A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures*, ACM Computing Surveys, 55(9), 2021, s. 1-38. https://doi.org/10.1145/3558001
3. Bandler, J., Merzon, A., *Cybercrime Investigations A Comprehensive Resource for Everyone*, Taylor & Francis Ltd, 2022.
4. Clarke, J., *SQL Injection Attacks and Defense*, Syngress, 2012.
5. Dimaggio, J., *Art of Cyberwarfare, An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*, No Starch Press,US, 2022.
6. Keplin, J., *Budowanie odporności państwa na działania hybrydowe*, Przegląd Bezpieczeństwa Wewnętrznego, nr 29(15), 2023, s. 13-38. https://doi.org/10.4467/20801335PBW.23.018.18760

7. Kitler, W., Chałubińska-Jentkiewicz, K., Badźmirowska-Masłowska, K., *System bezpieczeństwa w cyberprzestrzeni RP*, Towarzystwo Wiedzy Obronnej, 2018.
8. Kowalewski, M., Ochrona informacji i systemów teleinformatycznych w cyberprzeni, Oficyna Wydawnicza Politechniki Warszawskiej, 2017.
9. Kuś, B., *Siły Zbrojne Rzeczypospolitej Polskiej a cyberbezpieczeństwo. Zagadnienia organizacyjno-prawne*, Cybersecurity & Law, nr 2, 2023, s. 32-50.
10. Marczyk, M.M., Stolarz, M., Terebiński, B. (red.), *Cyberbezpieczeństwo: zagrożenia i wyzwania,* Mobilne sieci i systemy teleinformatyczne w cyberbezpieczeństwie Sił Zbrojnych RP, Wydawnictwo Akademii Sztuki Wojennej, Warszawa, 2023, s. 116-157.
11. Pollard, M., *A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States*, Pepperdine Policy Review: Vol. 16, Article 1, 2024.
12. Rais, R., Morillo, C., Gilman, E., Barth, D., *Zero Trust Networks: Building Secure Systems in Untrusted Network, 2nd Edition*, Helion, 2024.
13. Sallos, M.P., Garcia Perez, A., Bocanet, A., *Organisational cyber resilience: a heuristic for bridging foundations and applications*, Journal of Enterprise Information Management, 37(6), 2024, s. 1926-1952. https://doi.org/10.1108/JEIM-06-2023-0317
14. Serafin, M., *Bezpieczeństwo sieci firmowej. Kontrola ruchu wychodzącego*, Helion, 2022.
15. Sikorski, M., Honig, A., *Praktyczna Analiza Malware. Przewodnik po usuwaniu złośliwego oprogramowania*, Wydawnictwo Naukowe PWN, 2021.
16. Singh, A., *Military Computing Security: Insights and Implications*, Journal of Institution of Engineers (India): Series B, 104(3), 2023, s. 359-366.
17. Wrightson, T., *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization,* McGraw Hill, 2024.
18. Yaacoub, J.P., Noura, H.,Salman, O., Chehab, A., *Security analysis of drones systems: Attacks, limitations, and recommendations*, Internet of Things,11, 2020, 100218. https://doi.org/10.1016/j.iot.2020.100218
19. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2024, 2024.
20. GAO, *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon System*s, GAO-24-106221, Washington, DC: U.S. Government Accountability Office, 2024.
21. Ministerstwo Obrony Narodowej, *Resortowa strategia sztucznej inteligencji do roku 2039*, Warszawa, 2020.
22. NATO, *Allied Command Transformation (ACT)*, Cyber Resilience Strategic Concept. Norfolk, VA, 2023.
23. NATO, *Resilience as the first line of defence and deterrence*, NATO official publications, 2021.
24. NATO CCDCOE, *Locked Shields – The World's Largest and Most Complex International Live-Fire Cyber Defence Exercise*, 2025.
25. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, dokument rządowy, 2019.
26. Umowa między Stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych z 18.06.1964, (Dz. U. 2001.143.1594).

dr inż. Tomasz Grudniewski
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0003-3394-8992
https://doi.org/10.29316/9788368103199_8

ZAAWANSOWANE SYSTEMY FOTOWOLTAICZNE JAKO KLUCZOWY CZYNNIK WZMACNIAJĄCY BEZPIECZEŃSTWO ENERGETYCZNE PAŃSTWA

ADVANCED PHOTOVOLTAIC SYSTEMS AS A KEY FACTOR REINFORCING NATIONAL ENERGY SECURITY

Streszczenie

Rozdział przedstawia analizy i wnioski dotyczące roli zaawansowanych systemów fotowoltaicznych w kształtowaniu bezpieczeństwa energetycznego państwa. Wskazano, że rozwój nowoczesnych technologii PV, obejmujących m.in. wysokosprawne ogniwa, magazynowanie energii i inteligentne systemy sterowania, sprzyja dywersyfikacji źródeł, uniezależnieniu od importu paliw kopalnych oraz zwiększeniu odporności krajowej infrastruktury energetycznej. Rozdział analizuje wpływ zaawansowanych systemów fotowoltaicznych na bezpieczeństwo energetyczne państwa. Cel: Określenie, w jaki sposób nowoczesne technologie PV (m.in. wysokosprawne ogniwa, magazyny energii, inteligentne systemy

Summary

This paper examines the impact of advanced photovoltaic (PV) systems on a nation's energy security. Aim: To determine how modern PV technologies (including high-efficiency solar cells, energy storage, and intelligent control systems) can enhance a country's ability to ensure stable and resilient energy supplies. Research Problem: To what extent can advanced photovoltaics reduce dependence on fossil fuels, improve system resilience to disruptions (e.g., extreme weather events and cyberattacks), and help stabilize energy prices? Methods: The study applies a multi-faceted qualitative analysis based on a review of scientific literature and institutional reports (e.g., IEA,

sterowania) mogą wzmocnić zdolność państwa do zapewnienia stabilnych i odpornych dostaw energii. Problem: Czy i w jakim stopniu zaawansowana fotowoltaika zmniejsza zależność od paliw kopalnych, poprawia odporność systemu na zakłócenia (w tym ekstremalne zjawiska pogodowe i ataki cybernetyczne) oraz sprzyja stabilizacji cen energii? Metody: W rozdziale zastosowano wieloaspektową analizę jakościową, obejmującą przegląd literatury naukowej i raportów instytucjonalnych (m.in. IEA, IRENA), analizę danych statystycznych oraz studia przypadków. Porównano korzyści i potencjalne zagrożenia wynikające z rozwoju fotowoltaiki pod kątem bezpieczeństwa energetycznego, uwzględniając m.in. scenariusze kryzysowe, bariery surowcowe i nowe wyzwania regulacyjne.

Słowa kluczowe: zaawansowane systemy fotowoltaiczne, bezpieczeństwo energetyczne, odnawialne źródła energii

IRENA), statistical data analysis, and case studies. Benefits and potential risks related to PV development are compared from the perspective of energy security, accounting for crisis scenarios, material supply barriers, and emerging regulatory challenges.

Keywords: advanced photovoltaic systems, energy security, renewable energy sources

Wstęp

Bezpieczeństwo energetyczne jest jednym z kluczowych wymiarów polityki gospodarczej i narodowej, oznaczając zdolność państwa do zapewnienia nieprzerwanego dostępu do energii po akceptowalnej cenie oraz ochrony przed zakłóceniami dostaw[1]. Koncepcja ta tradycyjnie wiązała się z zabezpieczeniem dostaw paliw kopalnych (ropy, gazu, węgla) i stabilnością sieci elektroenergetycznej. Współcześnie nabiera ona nowego znaczenia w obliczu transformacji energetycznej i dążenia do gospodarki niskoemisyjnej. Rozwój odnawialnych źródeł energii, w tym energetyki słonecznej, oferuje szansę na zwiększenie bezpieczeństwa energetycznego poprzez dywersyfikację źródeł i uniezależnienie się od importowanych surowców. Jednocześnie transformacja ta wiąże się z nowymi wyzwaniami technologicznymi i geopolitycznymi, takimi jak zależność od dostaw komponentów i minerałów krytycznych czy konieczność zapewnienia elastyczności systemu z dużym udziałem źródeł

[1] International Energy Agency (IEA). Energy Security. [Online]. Dostęp: IEA Topics – Energy Security (2025).

zależnych od warunków pogodowych. Według raportu REN21, światowe inwestycje w odnawialne źródła energii wzrosły w 2022 roku do rekordowych 0,5 bln USD, co odzwierciedla priorytetowe traktowanie OZE jako elementu bezpieczeństwa energetycznego[2]. Fotowoltaika (PV) stała się w ostatnich dekadach jednym z najszybciej rozwijających się źródeł energii elektrycznej. Globalna moc zainstalowana PV przekroczyła 1,6 TW w 2023 roku (wzrost z 1,2 TW w 2022)[3], a energia słoneczna odpowiada już za ponad 5% światowej produkcji elektryczności[4]. Spadające koszty technologii – energia z dużych instalacji PV jest dziś najtańszym źródłem energii elektrycznej w wielu regionach – sprawiły, że fotowoltaika odgrywa główną rolę w nowych inwestycjach energetycznych[5]. Jednocześnie, wraz z rosnącym znaczeniem PV, pojawia się pytanie, w jaki sposób zaawansowane systemy fotowoltaiczne mogą przyczynić się do wzmocnienia bezpieczeństwa energetycznego państwa. Zaawansowane systemy fotowoltaiczne to pojęcie obejmujące nowoczesne technologie ogniw słonecznych, zintegrowane systemy magazynowania energii, inteligentne układy sterowania oraz innowacyjne zastosowania fotowoltaiki (np. agrifotowoltaika, systemy wyspowe, fotowoltaika zintegrowana z budynkami). Celem niniejszego rozdziału jest zbadanie, w jaki sposób takie zaawansowane rozwiązania fotowoltaiczne mogą stać się kluczowym czynnikiem wzmacniającym bezpieczeństwo energetyczne kraju. Wprowadzenie przedstawia ogólny kontekst bezpieczeństwa energetycznego i roli fotowoltaiki w transformacji energetycznej. W dalszych częściach zdefiniowano cel i problem badawczy, opisano zastosowane metody, dokonano przeglądu zaawansowanych technologii PV oraz przeanalizowano ich wpływ na różne aspekty bezpieczeństwa energetycznego (dywersyfikację dostaw, odporność systemu, niezależność energetyczną itp.), jak również zidentyfikowano wyzwania i wymagania związane z integracją fotowoltaiki na wielką skalę.

Celem rozdziału jest analiza wpływu zaawansowanych systemów fotowoltaicznych na bezpieczeństwo energetyczne państwa. W szczególności dążono do:

[2] REN21. Renewables 2023 Global Status Report. Paryż: REN21 Secretariat, 2023.

[3] IEA Photovoltaic Power Systems Programme (IEA-PVPS). Snapshot of Global PV Markets 2023. Report IEA-PVPS T1-42:2024, April 2024.

[4] A. K. Pandey, V. V. Tyagi, J. Selvaraj, N. A. Rahim, S. K. Tyagi, *Recent advances in solar photovoltaic systems for emerging trends and advanced applications*, Renewable and Sustainable Energy Reviews 53, 2016.

[5] International Energy Agency (IEA). Solar PV – Analysis and Forecasts 2023.

- scharakteryzowania najnowszych osiągnięć technologicznych w fotowoltaice oraz koncepcji zaawansowanych systemów PV (np. wysokosprawne ogniwa, magazyny energii, mikrosieci),
- oceny, w jaki sposób rozwój i wdrożenie tych rozwiązań może przyczynić się do wzmocnienia bezpieczeństwa energetycznego (rozumianego jako pewność, dostępność i odporność dostaw energii),
- zidentyfikowania głównych korzyści oraz potencjalnych ryzyk związanych z wysokim udziałem energii słonecznej w miksie energetycznym kraju,
- sformułowania rekomendacji dotyczących działań wspierających wykorzystanie zaawansowanej fotowoltaiki dla zwiększenia bezpieczeństwa energetycznego.

Realizacja powyższego celu wymagała zarówno studium literatury i danych empirycznych, jak i przeprowadzenia krytycznej analizy obecnych trendów technologicznych oraz politycznych związanych z energetyką słoneczną.

Główny problem badawczy podjęty w rozdziale można sformułować następująco: w jaki sposób zaawansowane systemy fotowoltaiczne wpływają na bezpieczeństwo energetyczne państwa i czy mogą stanowić kluczowy czynnik jego wzmocnienia? Innymi słowy, badanie koncentruje się na zależności między rozwojem nowoczesnej fotowoltaiki a zdolnością kraju do zabezpieczenia stabilnych, pewnych dostaw energii[6,7].

Szczegółowe pytania badawcze obejmują:

- Jakie innowacje technologiczne w obszarze fotowoltaiki (np. nowe materiały i konstrukcje ogniw, integracja z magazynami) zwiększają efektywność i niezawodność produkcji energii słonecznej?
- Czy i w jakim stopniu wysoki udział energetyki słonecznej może zastąpić tradycyjne źródła energii i ograniczyć zależność od importu paliw kopalnych?
- Jak zaawansowane systemy PV (np. systemy z magazynowaniem, mikroinstalacje prosumenckie, inteligentne sieci) wpływają na odporność

[6] Ch. Lamnatou, C. Cristofari, D. Chemisana. *Artificial Intelligence (AI) in relation to environmental life-cycle assessment, photovoltaics, smart grids and small-island economies*, Sustainable Energy Technologies and Assessments 71, 2024.

[7] S. Tsuchida, H. Nonaka, N. Yamada, *Deep Reinforcement Learning for the Optimal Angle Control of Tracking Bifacial Photovoltaic Systems,* Energies 15, 2022.

systemu elektroenergetycznego na zakłócenia (klęski żywiołowe, kryzysy geopolityczne, cyberataki)?
- Jakie bariery (techniczne, ekonomiczne, surowcowe) mogą ograniczać potencjał fotowoltaiki w kontekście bezpieczeństwa energetycznego i jak można im przeciwdziałać?

Rozwiązanie postawionego problemu badawczego ma dostarczyć odpowiedzi, czy zaawansowana fotowoltaika może pełnić rolę „bezpiecznika" krajowego systemu energetycznego w XXI wieku oraz jakie działania należy podjąć, aby potencjał ten w pełni wykorzystać.

Przeprowadzona praca ma charakter interdyscyplinarnej analizy łączącej perspektywę technologiczną i strategiczną. Zastosowano jakościową metodę badawczą opartą na przeglądzie literatury przedmiotu oraz danych wtórnych z raportów branżowych i analiz rządowych. W pierwszej fazie dokonano przeglądu aktualnych publikacji naukowych i raportów międzynarodowych instytucji (m.in. Międzynarodowej Agencji Energii – IEA, Międzynarodowej Agencji Energii Odnawialnej – IRENA) dotyczących[8,9]:

- definicji i czynników składowych bezpieczeństwa energetycznego (w tym klasycznych koncepcji „4A" – availability, accessibility, affordability, acceptability) oraz zmian podejścia do bezpieczeństwa energetycznego w dobie transformacji energetycznej[10],
- stanu rozwoju i trendów w technologii fotowoltaicznej (efektywności ogniw, kosztów, skali wdrożeń) na świecie[11],
- przykładów zastosowań zaawansowanych systemów PV (projekty pilotażowe, wdrożenia magazynów energii, mikrosieci z PV, systemy zwiększające odporność na awarie),
- badań nad wpływem rozwoju OZE (w szczególności PV) na wskaźniki bezpieczeństwa energetycznego państw[12].

[8] J. H. Sanchez, L. M. Castro, *Advanced three-stage photovoltaic system phasor model for grid integration dynamic studies*, Solar Energy, 235, 2022.

[9] H. Katir, A. Abouloifa, I. Lachkar, K. Noussi, F. Giri, J. M. Guerrero, *Advanced Nonlinear Control of A Grid-Connected Photovoltaic Power System Using N-Cascaded H-Bridge Multilevel Inverters*, IFAC PapersOnLine 53-2, 2020.

[10] International Energy Agency (IEA). *Energy Security*. [Online]. Dostęp: IEA Topics – Energy Security, 2025.

[11] International Energy Agency (IEA). Solar PV – Analysis and Forecasts, 2023.

[12] K. Khan, A. Khurshid, J. Cifuentes-Faura, D. Xianjun, *Does renewable energy development enhance energy security?* Utilities Policy, vol. 87, 2024.

W kolejnym etapie dokonano analizy porównawczej korzyści i ryzyk związanych z integracją fotowoltaiki w systemie energetycznym. Wykorzystano podejście analizy scenariuszowej, odnosząc się do sytuacji kryzysowych (np. nagłe przerwy dostaw paliw) i roli, jaką mogłaby odegrać generacja słoneczna. W tym celu przeanalizowano studia przypadków, m.in.:

- dane z Unii Europejskiej w okresie kryzysu gazowego 2021–2022, kiedy rekordowa generacja z PV latem 2022 pozwoliła zaoszczędzić znaczące wolumeny gazu ziemnego[13],
- inicjatywy zwiększania odporności systemu poprzez PV i magazyny energii (np. projekty mikrosieci na potrzeby wojskowe i infrastruktury krytycznej w USA)[14],
- programy wspierające integrację magazynowania z OZE (np. program SHINES Departamentu Energii USA[15], których celem jest stworzenie skalowalnych i opłacalnych systemów integrujących PV z magazynowaniem, zdolnych do niezawodnej pracy przy wysokim udziale OZE) oraz rozwiązania z zakresu inteligentnych sieci pozwalające na sterowanie popytem i podażą energii.

Zebrane informacje poddano krytycznej analizie, stosując metody wnioskowania dedukcyjnego. Na tej podstawie sformułowano syntezę dotyczącą wpływu zaawansowanej fotowoltaiki na bezpieczeństwo energetyczne oraz rekomendacje. W rozdziale wykorzystano również dwie ilustracje techniczne (rysunki) oraz dwie tabele zestawiające dane i wyniki analizy, celem lepszego zilustrowania omawianych zagadnień.

Zaawansowane technologie i systemy fotowoltaiczne

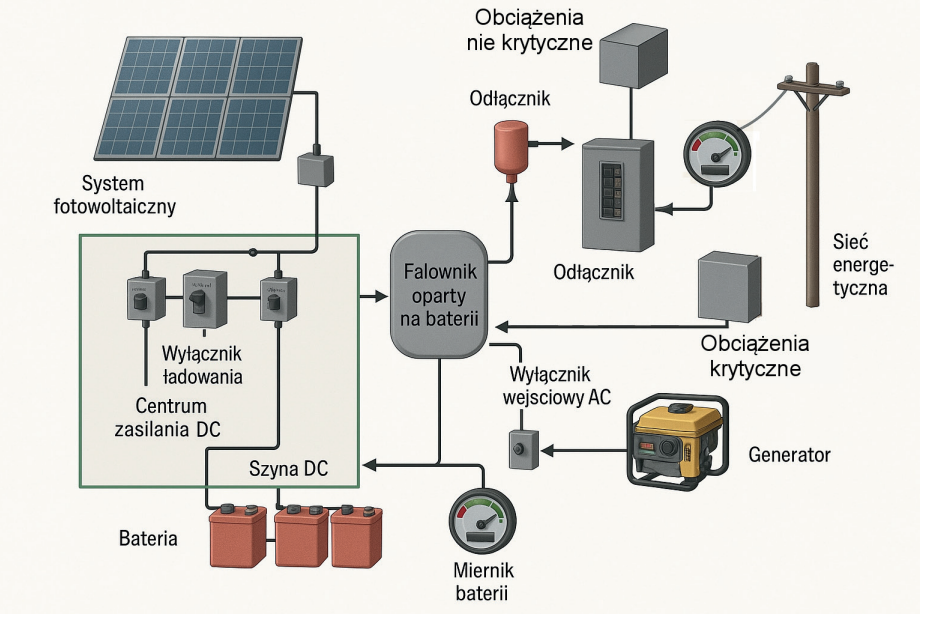
Dynamiczny rozwój technologii fotowoltaicznych w ostatnich latach doprowadził do powstania szeregu zaawansowanych rozwiązań PV, które charakteryzują się wyższą wydajnością, większą elastycznością zastosowań oraz lepszą integracją z siecią elektroenergetyczną. Poniżej omówiono wybrane kierunki postępu w fotowoltaice:

[13] V. Masterson, *Here's how solar energy saved Europeans $29 billion this summer*, World Economic Forum, 3 października 2022.

[14] American Council on Renewable Energy (ACORE). The Role of Renewable Energy in National Security. Issue Brief, October, 2018.

[15] U.S. Department of Energy (DOE). Sustainable and Holistic Integration of Energy Storage and Solar PV (SHINES). [Online] 2016.

- Nowe materiały i wysokosprawne ogniwa PV: Tradycyjne krystaliczne ogniwa krzemowe, dominujące na rynku, osiągnęły sprawności rzędu 20–22% w produkcji masowej, a rekord laboratoryjny przekroczył 26%. Obecnie intensywnie rozwijane są ogniwa wielozłączowe oraz tandemowe, łączące krzem z innymi półprzewodnikami. Przykładem jest tandem perowskitowo-krzemowy, w którym warstwa perowskitu uzupełnia widmo absorpcji krzemu. Najnowsze prototypy tego typu ogniw osiągnęły sprawność konwersji na poziomie 34,6%[16], przekraczając teoretyczny limit pojedynczego złącza i znacząco przewyższając wydajność konwencjonalnych ogniw krzemowych. Rysunek 1 ilustruje schemat zaawansowanego systemu PV zintegrowanego z magazynem energii, pozwalającego na bardziej stabilną generację energii.



Rysunek 1. Schemat zaawansowanego systemu fotowoltaicznego z magazynem energii, umożliwiającego pracę wyspową dla odbiorów krytycznych
Źródło: opracowanie własne.

Oprócz tandemów perowskitowych rozwijane są ogniwa z arsenku galu i innych półprzewodników III-V, często w układach wielozłączowych

[16] V. Shaw, E. Bellini, *Longi achieves 34.6% efficiency for two-terminal tandem perovskite solar cell prototype*, PV Magazine International, 2024.

stosowanych pod koncentratorami światła – osiągnęły one rekordowe sprawności ponad 45% (w warunkach koncentracji), choć na razie wykorzystuje się je głównie w zastosowaniach kosmicznych ze względu na wysoki koszt. Równolegle udoskonalane są technologie cienkowarstwowe (np. CdTe, CIGS), które choć ustępują krzemowi pod względem sprawności (komercyjnie ok. 15-18%), oferują inne zalety – niższy koszt jednostkowy w niektórych zastosowaniach i lepsze działanie w rozproszonym świetle. Rozwój zaawansowanych modeli i narzędzi AI znacząco usprawnia projektowanie i optymalizację ogniw PV[17,18].

- Magazynowanie energii i hybrydowe systemy PV: Samodzielne systemy fotowoltaiczne generują energię w sposób zależny od nasłonecznienia (z cyklem dziennym i sezonowym), co stanowi wyzwanie dla bilansowania sieci. Wprowadzenie magazynów energii (najczęściej w postaci baterii litowo-jonowych) w zaawansowanych instalacjach PV umożliwia gromadzenie nadwyżek energii w okresach wysokiej produkcji i wykorzystywanie ich w godzinach braku słońca. Dzięki temu energia słoneczna staje się bardziej dyspozycyjna – może pokrywać zapotrzebowanie również wieczorem czy w nocy, zwiększając pewność zasilania. Technologie takie są rozwijane m.in. w ramach programów typu SHINES (Sustainable and Holistic Integration of Energy Storage and Solar PV) Departamentu Energii USA[19], których celem jest stworzenie skalowalnych i opłacalnych systemów integrujących PV z magazynowaniem, zdolnych do niezawodnej pracy przy wysokim udziale OZE. Coraz częściej duże farmy fotowoltaiczne budowane są od razu jako *systemy hybrydowe PV+magazyn*, co pozwala operatorom oferować usługę zbliżoną charakterem do elektrowni konwencjonalnej – dostarczanie mocy według zapotrzebowania, a nie tylko w trybie pasywnym zależnym od pogody. W ostatnich latach

[17] H. Togun, A. Basem, M. J. Jweeg, N. Biswas, A. M. Abed, D. Paul, H. I. Mohammed, A. Chattopadhyay, B. K. Sharma, T. Abdulrazzaq, *Advancing organic photovoltaic cells for a sustainable future: The role of artificial intelligence (AI) and deep learning (DL) in enhancing performance and innovation*, Solar Energy, 291, 2025.

[18] R. Abbassi, S. Saidi, H. Jerbi, L. Ladhar, M. Omri, *Accurate parameters extraction of photovoltaic models using Lambert W-function collaborated with AI-based Puma optimization method*, Results in Engineering, 25, 2025.

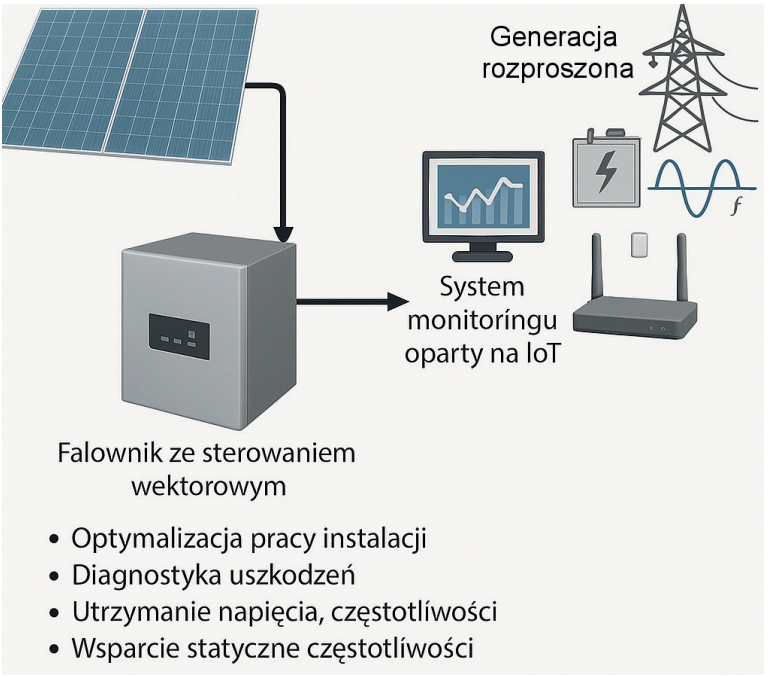
[19] U.S. Department of Energy (DOE). Sustainable and Holistic Integration of Energy Storage and Solar PV (SHINES). [Online]. 2016.

pojawiają się systemy kojarzące fotowoltaikę z akumulacją energii cieplnej bądź sprężonego powietrza, sterowane narzędziami AI[20,21].

- Inteligentne systemy sterowania i monitoringu: Zaawansowane systemy PV wyposażone są w nowoczesne układy energoelektroniczne (np. falowniki ze sterowaniem wektorowym – rysunek 2) oraz systemy monitoringu oparte na IoT. Pozwala to na bieżącą optymalizację pracy instalacji, diagnostykę uszkodzeń, a także udział generacji rozproszonej w usługach regulacyjnych sieci (utrzymanie napięcia, częstotliwości). Przykładowo, *inteligentne falowniki* mogą automatycznie redukować moc lub przesuwać punkt pracy ogniw, aby zapobiegać przeciążeniom sieci lokalnej, oraz dostarczać usługę *statycznego wsparcia częstotliwości* przez chwilowe oddawanie energii zgromadzonej w kondensatorach. Zaawansowane systemy nadzoru umożliwiają też szybkie reagowanie na awarie – monitorując tysiące modułów można z wyprzedzeniem wykrywać anomalie wskazujące np. na degradację paneli czy problemy z okablowaniem. Ponadto, integracja z systemami zdalnego sterowania (SCADA) i wykorzystanie algorytmów sztucznej inteligencji do prognozowania nasłonecznienia zwiększa przewidywalność i efektywność wykorzystania PV.

[20] J. Brinkley, L. Jiang, B. Widyolar, S. K. Hota, Y. Bhusal, G. Diaz, R. Winston, *Thermal, electrical, and cost study of advanced optical photovoltaic thermal system (ADOPTS)*, Applied Energy, 269, 2020.

[21] E. Assareh, A. Keykhah, A. Bedakhanian, N. Agarwal, M. Lee, *Optimizing solar photovoltaic farm-based cogeneration systems with artificial intelligence (AI) and Cascade compressed air energy storage for stable power generation and peak shaving: A Japan-focused case study*, Applied Energy, 377, 2025.



Rysunek 2. Schemat zaawansowanego systemu fotowoltaicznego z falownikiem ze sterowaniem wektorowym)

Źródło: opracowanie własne.

- Innowacyjne aplikacje fotowoltaiki: W zakresie zastosowań fotowoltaika wykracza poza tradycyjne farmy naziemne i dachowe systemy prosumenckie. Pojawiają się systemy agrofotowoltaiczne, łączące produkcję rolną z energią (panele nad uprawami), fotowoltaika zintegrowana z infrastrukturą (np. panele jako elementy fasad budynków, ekranów akustycznych, zadaszeń parkingów) oraz pływające farmy PV na zbiornikach wodnych, zmniejszające problem zajmowania cennych gruntów. Te innowacje poszerzają możliwości implementacji PV, przyczyniając się do zwiększenia potencjału generacji słonecznej w skali kraju. Co istotne, wiele z tych rozwiązań sprzyja rozproszeniu źródeł – np. instalacje BIPV (Building Integrated PV) umożliwiają włączenie produkcji energii w strukturę miast, co ma znaczenie dla odporności systemu (trudniej o awarię jednocześnie wszystkich rozproszonych źródeł).

Tabela 1 przedstawia porównanie wybranych zaawansowanych technologii fotowoltaicznych pod kątem ich sprawności i charakterystyki. Zestawienie to obrazuje, że osiągane obecnie w laboratoriach sprawności znacząco

przekraczają dotychczasowe standardy komercyjne, co otwiera drogę do przyszłych, jeszcze wydajniejszych systemów PV.

Tabela 1. Charakterystyka wybranych technologii ogniw fotowoltaicznych

Technologia PV	Sprawność lab. (rekord)	Sprawność komercyjna	Status i zastosowania
Monokrystaliczny krzem (c-Si)	ok. 26,7%	20–22%	Dominująca na rynku, dojrzała technologia; dalsze ulepszenia poprzez ogniwa typu PERC, TOPCon, HJT.
Cienkowarstwowa (CdTe, CIGS)	ok. 22%	15–18%	Tańsze materiały, niższa sprawność; stosowane głównie w farmach wielkopowierzchniowych.
Tandem perowskit + c-Si	33–35%	~30% (pilotażowo)	Technologia w fazie badań i wdrożeń demonstracyjnych; duży potencjał wzrostu sprawności modułów.
Wielozłączowe III-V (koncentrator)	>45% (koncentracja)	~30–35% (bez koncentr.)	Najwyższe sprawności przy skoncentrowanym świetle; zastosowania specjalistyczne (kosmos, CPV).

Źródło: opracowanie własne na podstawie danych NREL, PV Magazine i komunikatów producentów[22,23].

Warto podkreślić, że ciągły postęp technologiczny w fotowoltaice przekłada się nie tylko na wyższą efektywność konwersji energii promieniowania słonecznego, ale także na obniżenie kosztów oraz wzrost niezawodności systemów. W latach 2010-2023 średni koszt energii z instalacji PV spadł o kilkadziesiąt procent, co czyni fotowoltaikę jednym z najbardziej konkurencyjnych źródeł energii[24]. Dzięki temu kraje mogą szybciej zwiększać swój potencjał mocy słonecznej, co – jak omówiono w następnych sekcjach – ma istotne implikacje dla bezpieczeństwa energetycznego.

Fotowoltaika a bezpieczeństwo energetyczne państwa

Rozwój energetyki słonecznej wpływa na bezpieczeństwo energetyczne państwa w wielu wymiarach. Poniżej przeanalizowano, jak zaawansowane systemy fotowoltaiczne przyczyniają się do wzmocnienia (oraz jakie stwarzają

[22] International Energy Agency (IEA). Energy Security. [Online]. Dostęp: IEA Topics – Energy Security, 2025.

[23] V. Shaw, E. Bellini, *Longi achieves 34.6% ...*, op. cit.

[24] International Energy Agency (IEA). Solar PV – Analysis and Forecasts 2023. [Online]. IEA, 2024.

wyzwania dla) bezpieczeństwa energetycznego, odnosząc się do głównych składowych tego pojęcia.

Dywersyfikacja źródeł energii i niezależność od importu. Tradycyjnie bezpieczeństwo energetyczne było zagrożone przez nadmierną zależność od importowanych paliw kopalnych. Wprowadzenie znaczącego udziału krajowej energii słonecznej do miksu zmniejsza tę zależność. Fotowoltaika korzysta z *niewyczerpalnego, lokalnego zasobu*, jakim jest promieniowanie słoneczne – w przeciwieństwie do paliw, których zasoby są skoncentrowane geograficznie i podlegają wahaniom podaży na rynkach światowych. Każda megawatogodzina energii wyprodukowana ze słońca to odpowiednio mniej zużytego gazu czy węgla, co przekłada się na mniejszą wrażliwość państwa na szoki podażowe i skoki cen surowców. Przykładowo, w Unii Europejskiej rekordowa generacja słoneczna latem 2022 (99,4 TWh w okresie maj–sierpień) pozwoliła uniknąć zakupu ok. 20 mld m³ gazu ziemnego, co odpowiadało oszczędności około 29 mld USD[25]. Było to kluczowe w obliczu kryzysu wywołanego ograniczeniem dostaw z Rosji – energia słoneczna złagodziła niedobory i wysokie ceny gazu. Rządy wielu państw zauważyły tę rolę PV: polityki UE (np. plan REPowerEU) zakładają przyspieszenie inwestycji w OZE jako element uniezależnienia się od importu paliw z niestabilnych kierunków.

Dostępność i pewność dostaw energii. Bezpieczeństwo energetyczne to nie tylko kwestia geopolityki dostaw, ale także zdolność do pokrycia krajowego zapotrzebowania na energię w sposób ciągły, nawet w sytuacjach nadzwyczajnych. Rozproszone systemy fotowoltaiczne zwiększają *dyspozycyjność mocy* w kraju poprzez dodanie wielu niezależnych źródeł generacji. W odróżnieniu od wielkich elektrowni, których awaria lub wyłączenie (np. z powodu usterki albo ataku) może pozbawić system znaczącej części mocy, setki tysięcy rozsianych instalacji PV tworzą system bardziej *modularny i odporny*. Uszkodzenie pojedynczych instalacji (np. wskutek ekstremalnej pogody) ma relatywnie niewielki wpływ na całość generacji słonecznej. Dodatkowo, fotowoltaika może funkcjonować w skali mikro – zasilając *mikrosieci* lub obiekty autonomiczne. Takie rozwiązania są szczególnie cenne dla zasilania infrastruktury krytycznej w sytuacjach kryzysowych. Na przykład baza wojskowa lub szpital wyposażony we własną elektrownię PV z magazynem może zachować zasilanie nawet w razie blackoutu w sieci głównej. Już w 2018 r. Pentagon

[25] V. Masterson, *Here's how solar energy saved Europeans $29 billion this summer*, World Economic Forum, 2022.

wskazywał, że łączenie odnawialnych źródeł z magazynami w formie samowystarczalnych mikro-sieci zwiększa odporność operacyjną baz wojskowych i stanowi element bezpieczeństwa narodowego USA[26].

Stabilność cenowa i dostępność ekonomiczna energii. IEA definiuje bezpieczeństwo energetyczne także poprzez kryterium *przystępności cenowej* energii[27]. W tym kontekście fotowoltaika odgrywa pozytywną rolę, gdyż nie generuje kosztów paliwa – raz zainstalowane moduły produkują energię praktycznie za darmo przez 25 i więcej lat. To chroni odbiorców przed ryzykiem gwałtownych wzrostów cen paliw kopalnych. Doświadczenie z lat 2021–2022, gdy ceny gazu i węgla na rynkach światowych gwałtownie wzrosły, pokazuje, że kraje z większym udziałem OZE były mniej narażone na przenoszenie się tych wzrostów na ceny energii dla przemysłu i gospodarstw domowych. Energia słoneczna działa zatem stabilizująco na rynek – zwiększając podaż energii o niskim koszcie krańcowym, obniża hurtowe ceny energii elektrycznej w okresach wysokiej generacji (zjawisko tzw. *merit order effect*). Co więcej, inwestycje w fotowoltaikę są coraz bardziej opłacalne rynkowo – w wielu regionach świata koszt produkcji 1 kWh z PV jest obecnie niższy niż z nowych elektrowni węglowych czy gazowych[28]. Dla państwa oznacza to mniejsze obciążenie bilansu handlowego (mniej wydatków na import paliw) oraz korzyści dla gospodarki poprzez rozwój nowego sektora technologicznego.

Odporność infrastruktury energetycznej. Rosnąca częstotliwość ekstremalnych zjawisk pogodowych (burze, fale upałów, mrozy) oraz zagrożenia takie jak cyberataki każą zwracać uwagę na *odporność* (resilience) systemu energetycznego. Zaawansowane systemy PV mogą tę odporność zwiększać, o ile są odpowiednio projektowane. Badania wykazały, że instalacje fotowoltaiczne mogą przetrwać nawet gwałtowne zjawiska – np. w kampusie NREL w Kolorado gradobicie w 2017 r. uszkodziło tylko 1 z 3000 paneli[29]. Kluczowe jest jednak posiadanie lokalnych źródeł energii na wypadek rozległych awarii sieci – i tu rozproszone PV wraz z magazynami stanowią rozwiązanie. Np. portorykańskie projekty *solarnych mikrosieci* były rozwijane po huraganie

[26] American Council on Renewable Energy (ACORE). The Role of Renewable Energy in National Security. Issue Brief, October 2018.

[27] International Energy Agency (IEA). Energy Security. [Online]. Dostęp: IEA Topics – Energy Security, 2025.

[28] American Council on Renewable Energy (ACORE). The Role of Renewable Energy in National Security. Issue Brief, 2018.

[29] National Renewable Energy Laboratory (NREL). Resilient Solar Photovoltaics. [Online]. Dostęp: NREL Security & Resilience, 2024.

Maria, aby społeczności lokalne mogły szybciej odzyskać zasilanie po klęsce żywiołowej. Rysunek 3 pokazuje przykładową niewielką instalację dachową PV w budynku jednorodzinnym – takie mikroinstalacje, w połączeniu z magazynem, zwiększają indywidualne bezpieczeństwo energetyczne gospodarstw domowych, ograniczając ich zależność od zewnętrznej sieci. Z punktu widzenia odporności, ważnym aspektem jest także *cyberbezpieczeństwo*. Paradoksalnie, rozproszenie źródeł zmniejsza ryzyko fizycznych zniszczeń, ale pojawia się nowe zagrożenie – tysiące inteligentnych urządzeń sterujących PV mogą stać się celem ataku hakerskiego. Jeśli są one połączone w sieci i sterowane zdalnie, skoordynowany atak mógłby zakłócić ich pracę. Eksperci ostrzegają, że przy wysokim udziale fotowoltaiki potencjalny cyberatak wyłączający dużą liczbę falowników mógłby doprowadzić do znacznych niedoborów energii elektrycznej[30]. Dlatego rozwój zaawansowanych systemów PV musi iść w parze z zabezpieczeniami informatycznymi i protokołami chroniącymi przed przejęciem kontroli nad urządzeniami (szyfrowana komunikacja, standardy bezpieczeństwa IoT, możliwość odizolowania i ręcznego sterowania w razie incydentu). Wymaga to nowych regulacji i standardów – rządy już dostrzegają ten problem i zaczynają opracowywać wytyczne dla cyberbezpieczeństwa OZE.



Rysunek 3. Przykładowa mikroinstalacja fotowoltaiczna prosumencka na dachu budynku mieszkalnego

Źródło: opracowanie własne.

[30] *Panele fotowoltaiczne potencjalną furtką dla cyberprzestępców?* Energetyka24.com, 2021.

Akceptowalność środowiskowa i społeczna. Bezpieczeństwo energetyczne bywa definiowane również poprzez *akceptowalność społeczną* źródeł energii (np. w ramach koncepcji 4A uwzględnia się „acceptability")[31]. Fotowoltaika jako czyste źródło energii sprzyja bezpieczeństwu w długim horyzoncie poprzez ograniczanie zmian klimatu – a te stanowią rosnące zagrożenie dla stabilności dostaw energii (np. susze zagrażające energetyce wodnej, ocieplenie wpływające na zapotrzebowanie szczytowe). Redukcja emisji CO2 dzięki PV (w Polsce 1 kWh z PV to ok. 700 g CO2 mniej w porównaniu z węglem) przyczynia się zatem pośrednio do łagodzenia ryzyka klimatycznego. Ponadto, energia słoneczna cieszy się na ogół wysoką akceptacją społeczną – instalacje PV są postrzegane jako nieuciążliwe, bezpieczne i korzystne dla lokalnych społeczności (w przeciwieństwie np. do obaw związanych z energetyką jądrową czy wydobyciem gazu łupkowego). To ułatwia rozwój fotowoltaiki i zmniejsza napięcia społeczne wokół infrastruktury energetycznej, co również jest elementem bezpieczeństwa (mniejsze ryzyko protestów, wstrzymania inwestycji itp.).

Powyższe punkty pokazują wielowymiarowy pozytywny wpływ PV na bezpieczeństwo energetyczne. Dla pełnego obrazu należy jednak rozważyć także ograniczenia i warunki, od których spełnienia zależy realne wykorzystanie tego potencjału.

Wyzwania integracji fotowoltaiki w systemie energetycznym

Mimo licznych zalet, duży wzrost udziału fotowoltaiki w systemie niesie też wyzwania, które należy adresować, aby nie osłabiły one bezpieczeństwa energetycznego. Do najważniejszych należą:

- Zmienność i nieprzewidywalność generacji: Produkcja PV zależy od pory dnia i warunków pogodowych, co oznacza, że bezpośrednio nie zapewnia ciągłości dostaw przez 24 godziny na dobę. Przy wysokiej penetracji PV system wymaga odpowiednich mechanizmów równoważenia – elastycznych rezerw mocy, magazynów energii lub sterowania popytem. Brak takich środków mógłby skutkować niedoborami mocy w nocy lub w pochmurne dni. Na szczęście rozwój technologii magazynowania energii postępuje szybko – koszt baterii spada, a ich zastosowanie

[31] International Energy Agency (IEA). Energy Security. [Online]. Dostęp: IEA Topics – Energy Security, 2025.

jest kluczowe dla zapewnienia stabilności dostaw[32]. Również *zarządzanie popytem* (DSM) i zwiększenie elastyczności po stronie odbiorców może zmniejszyć to ryzyko (np. programy zachęcające do zużycia energii w środku dnia, gdy pracuje PV). Przyszły bezpieczny system energetyczny z dużym udziałem słońca wymaga więc równoległych inwestycji w magazyny i inteligentną infrastrukturę sieciową.

- Potrzeba rozbudowy i modernizacji sieci: Generacja słoneczna jest często zlokalizowana w innych punktach niż tradycyjne elektrownie (np. na niższych poziomach napięć rozdzielczych). Aby bezpiecznie zasilać system, sieci przesyłowe i dystrybucyjne muszą być dostosowane do dwukierunkowych przepływów energii i zmiennych poziomów obciążenia. Konieczne są inwestycje w infrastrukturę (transformatory, linie, systemy sterowania), by uniknąć przeciążeń i zapewnić możliwość odbioru mocy ze słońca w okresach jej szczytu. Wymaga to nakładów finansowych i planowania przestrzennego (np. budowy farm PV tam, gdzie sieć ma wystarczające moce przesyłowe lub ich wzmocnienia tam, gdzie powstają nowe duże inwestycje PV).
- Zależność od dostaw komponentów i surowców: Paradoksalnie, uniezależniając się od importu ropy czy gazu, państwa mogą popaść w nową zależność – od importu paneli fotowoltaicznych, baterii lub surowców do ich produkcji. Obecnie ok. 80-90% globalnych mocy produkcyjnych modułów PV znajduje się w jednym kraju (Chiny). Taka koncentracja łańcucha dostaw stanowi potencjalne ryzyko geopolityczne (np. cła, ograniczenia eksportowe, zakłócenia transportu). Ponadto produkcja paneli wymaga szeregu *minerałów krytycznych* – krzemu wysokiej czystości, srebra (na elektrody), indu, telluru (dla niektórych technologii cienkowarstwowych), a magazyny energii potrzebują litu, kobaltu, niklu itp. IEA ostrzega, że przy obecnych trendach popyt na te surowce dla energetyki odnawialnej wzrośnie wielokrotnie, grożąc niedoborami, jeśli nie zwiększą się inwestycje w ich wydobycie i przetwórstwo[33]. Dla bezpieczeństwa energetycznego istotna jest zatem strategia zapewnienia dostępu do tych kluczowych materiałów – poprzez dywersyfikację dostaw, rozwój własnych mocy produkcyjnych (np. fabryk paneli w kraju lub regionie),

[32] D. Papathanasiou, *Why energy storage matters for the global energy transition*, *World Bank Blogs*, 2023.

[33] International Energy Agency (IEA). The Role of Critical Minerals in Clean Energy Transitions. Paryż: IEA, 2021.

a także recykling zużytych instalacji w przyszłości. Unia Europejska już podejmuje działania w tym kierunku, ogłaszając inicjatywy na rzecz rozwoju rodzimego przemysłu PV i łańcuchów dostaw (np. European Solar Initiative).

- Wymogi regulacyjne i rynkowe: Aby zaawansowane systemy PV mogły faktycznie wzmocnić bezpieczeństwo systemu, potrzebne są odpowiednie ramy prawne i rynkowe. Przykładowo, usługi systemowe (rezerwa mocy, regulacja częstotliwości) muszą być tak zdefiniowane, aby mogły je świadczyć jednostki OZE z magazynami lub agregatorzy wielu mikroinstalacji (w formie *wirtualnych elektrowni*). Operatorzy systemów muszą z kolei zmienić podejście do planowania – więcej uwagi wymaga prognozowanie produkcji z OZE i zarządzanie ryzykiem pogodowym. W wielu krajach konieczne okazało się także dostosowanie struktur taryfowych i zasad rynku energii, by zachęcać do instalacji magazynów i elastyczności (np. taryfy czasowe, kontrakty typu PPA zapewniające stabilne ceny energii z PV dla odbiorców). Brak takich dostosowań mógłby hamować rozwój zaawansowanej fotowoltaiki lub prowadzić do problemów z bilansowaniem, co w efekcie zagrażałoby stabilności dostaw.

Tabela 2 syntetycznie porównuje konwencjonalny system oparty na paliwach kopalnych z systemem zdominowanym przez fotowoltaikę pod kątem kilku kluczowych aspektów bezpieczeństwa energetycznego.

Tabela 2. Porównanie wybranych aspektów bezpieczeństwa energetycznego w systemie tradycyjnym (paliw kopalnych) i systemie z dominującą fotowoltaiką

Aspekt	System konwencjonalny (kopalne)	System zdominowany przez PV
Zależność od surowców	Import paliw (ropa, gaz); ryzyko geopolitycznych zakłóceń	Zasoby lokalne (słońce); brak paliwa do importu
Ciągłość dostaw	Ciągła praca elektrowni, ale ryzyko awarii dużej jednostki	Zmienna generacja (dzień/noc); wymaga magazynów i rezerw
Koszty zmienne	Wysokie koszty paliwa, podatne na wahania cen	Brak kosztu paliwa; stabilne koszty operacyjne
Odporność na awarie	Uszkodzenie rafinerii/elektrowni poważne dla systemu	Rozproszona generacja; awarie lokalne mniej groźne
Infrastruktura sieci	Układ scentralizowany, przepływ jednostronny	Wymaga modernizacji dla dwukierunkowych przepływów i integracji prosumentów
Emisyjność	Wysoka (CO_2, zanieczyszczenia powietrza)	Znikoma podczas generacji; efekt klimatyczny pozytywny
Zagrożenia nowe	Zagrożenia fizyczne dostaw (ataki na infrastrukturę)	Zagrożenia cyfrowe (cyberataki na inteligentne systemy)

Źródło: opracowanie własne.

Jak wynika z Tabeli 2, przejście od systemu konwencjonalnego do opartego na fotowoltaice znacząco zmienia profil ryzyka i charakter bezpieczeństwa energetycznego – większość zmian działa na korzyść (mniejsza zależność od importu, brak kosztów paliwa, niższe emisje), pojawiają się jednak nowe wyzwania (konieczność zapewnienia elastyczności, cyberbezpieczeństwo, zabezpieczenie łańcuchów dostaw technologii).

Wnioski

Przeprowadzona analiza wskazuje, że zaawansowane systemy fotowoltaiczne mogą pełnić rolę kluczowego filaru bezpieczeństwa energetycznego państwa, pod warunkiem podjęcia działań towarzyszących umożliwiających pełne wykorzystanie ich potencjału. Państwa, które wcześnie zainwestowały w rozwój OZE, czerpią już konkretne korzyści bezpieczeństwotwórcze. Dobrym przykładem jest transformacja energetyczna Niemiec – duży udział PV i wiatru znacząco obniżył import gazu w sektorze elektroenergetycznym, a jednocześnie zdywersyfikował miks energetyczny, utrudniając zastosowanie „broni energetycznej" przez dostawców surowców. Z kolei kraje takie jak, Dania czy Australia, gdzie udział fotowoltaiki (i generalnie OZE) w produkcji prądu sięga kilkudziesięciu procent, wypracowały rozwiązania integracyjne: systemy aukcyjne i magazynowe, mechanizmy wymiany międzysystemowej, które pozwalają zarządzać zmiennością źródeł odnawialnych bez utraty stabilności dostaw.

Istotnym wnioskiem z badań jest potwierdzenie tezy, że bezpieczeństwo energetyczne w erze odnawialnej wymaga myślenia *wielowymiarowego* i uwzględnienia nowych czynników. O ile dawniej dominowało podejście polegające na zabezpieczaniu szlaków dostaw ropy czy utrzymywaniu rezerw strategicznych paliw, o tyle dziś równorzędne znaczenie ma zabezpieczenie łańcuchów dostaw technologii (np. dostępność paneli, inwerterów, komponentów elektronicznych), jak również zdolność do zapewnienia elastyczności popytowo-podażowej (np. poprzez sieci inteligentne i magazyny energii). Polityka energetyczna musi więc rozszerzyć tradycyjne środki (magazynowanie ropy, dywersyfikacja dostaw gazu) o nowe elementy: wsparcie dla przemysłu OZE, inwestycje w badania nad alternatywami surowcowymi (recykling, zastępowanie rzadkich pierwiastków w konstrukcji paneli) oraz rozwój *międzynarodowych partnerstw technologicznych* zapewniających wymianę know-how i dostęp do komponentów. IRENA w swoim raporcie

„Geopolitics of the Energy Transformation" podkreśla, że w systemach opartych na odnawialnych źródłach dominującą rolę odgrywać będzie technologia, a nie paliwa – stąd odporność łańcuchów dostaw technologii staje się niezbędnym elementem bezpieczeństwa energetycznego. Podobnie Międzynarodowa Agencja Energii w raporcie World Energy Outlook 2022 przedstawiła dziesięć zasad wzmacniania bezpieczeństwa energetycznego w trakcie transformacji – nacisk położono na synchronizację przyspieszonego rozwoju czystych technologii z odchodzeniem od paliw kopalnych oraz na inwestycje w elastyczność i efektywność, aby przejście do systemu opartego na OZE było płynne i bezpieczne[34].

Z perspektywy strategicznej, zaawansowana fotowoltaika wpisuje się w koncepcję tzw. *bezpieczeństwa wielowymiarowego*. Jej rozwój jednocześnie wzmacnia filary klasyczne (dostępność i ciągłość dostaw), jak i wpisuje się w cele zrównoważonego rozwoju (łagodzenie zmian klimatu). W dobie, gdy zagrożenia dla bezpieczeństwa mogą wynikać z czynników ekologicznych czy pandemii (zaburzającej łańcuchy dostaw), posiadanie niezależnych, czystych źródeł energii stanowi element budowania odporności państwa na różnorodne kryzysy. Należy zauważyć, że przeprowadzone rozważania mają charakter ogólny i syntetyczny. Poszczególne aspekty wymagają pogłębionych badań ilościowych – np. modelowania systemowego określającego, ile MW magazynów potrzeba na każde 100 MW PV, by utrzymać wymagany poziom rezerwy mocy; czy analiz ekonomicznych optymalnego miksu źródeł. Niemniej, już teraz dostępne dane empiryczne potwierdzają kierunek wniosków: odnawialne źródła energii wzmacniają bezpieczeństwo energetyczne poprzez redukcję ryzyk starych (geopolitycznych, ekonomicznych), wprowadzając zarazem nowe wyzwania, którym jednak można sprostać poprzez odpowiednią politykę i postęp techniczny[35].

Podsumowanie

Zaawansowane systemy fotowoltaiczne stanowią obecnie jeden z najważniejszych czynników kształtujących przyszłe bezpieczeństwo energetyczne. Jak wykazano w rozdziale, szerokie wykorzystanie energii słonecznej – wsparte nowoczesnymi technologiami magazynowania i inteligentnego

[34] International Energy Agency (IEA). World Energy Outlook 2022. Paryż: IEA, 2022.

[35] K. Khan, A. Khurshid, J. Cifuentes-Faura, D. Xianjun, *Does renewable energy development enhance energy security?* Utilities Policy, vol. 87, 2024.

zarządzania – może znacząco podnieść zdolność państwa do samodzielnego zaspokojenia zapotrzebowania na energię w sposób stabilny, zrównoważony i odporny na zakłócenia. Do głównych korzyści zalicza się zwiększenie niezależności od zewnętrznych dostaw paliw (a tym samym ograniczenie wpływu napięć geopolitycznych na krajową energetykę), poprawę odporności infrastruktury dzięki rozproszeniu źródeł oraz stabilizację kosztów energii dla gospodarki. Z drugiej strony, transformacja w kierunku systemu opartego na fotowoltaice wymaga przezorności i inwestycji towarzyszących. Należy zabezpieczyć dostawy krytycznych materiałów i komponentów do budowy instalacji PV (poprzez dywersyfikację partnerów handlowych i rozwój rodzimego przemysłu). Konieczne jest również wdrożenie mechanizmów gwarantujących bilansowanie systemu – co obejmuje rozwój magazynów energii na szeroką skalę, interkonektorów międzysystemowych pozwalających dzielić się nadwyżkami OZE z sąsiadami, a także cyfrowych narzędzi zarządzania popytem. Wreszcie, cyberbezpieczeństwo i standaryzacja inteligentnych urządzeń muszą stać się integralną częścią strategii energetycznej.

Podsumowując, zaawansowana fotowoltaika pełni rolę katalizatora zmian sprzyjających bezpieczeństwu energetycznemu – ale jej pozytywny efekt nie zrealizuje się automatycznie. Wymaga to świadomej polityki: wspierania innowacji (aby nowe rekordy sprawności szybko przekładały się na komercyjne produkty), inwestycji w infrastrukturę oraz edukacji i akceptacji społecznej dla nowych rozwiązań (np. prosumenci, mikrosieci). Państwa, które odpowiednio wcześnie i kompleksowo wdrożą te działania, zyskają podwójnie: zapewnią sobie bezpieczeństwo dostaw energii oraz odegrają wiodącą rolę w globalnej transformacji energetycznej, czerpiąc z tego również korzyści gospodarcze.

Ostatecznym wnioskiem płynącym z przeprowadzonej analizy jest stwierdzenie, że fotowoltaika – wspierana przez zaawansowane technologie – nie tylko przyczynia się do dekarbonizacji, ale też staje się filarem bezpieczeństwa energetycznego nowoczesnego państwa. W dobie wyzwań klimatycznych i geopolitycznych, inwestycja w słońce okazuje się inwestycją w bezpieczeństwo i suwerenność energetyczną.

Literatura

1. Abbassi R., Saidi S., Jerbi H., Ladhar L., Omri M., *Accurate parameters extraction of photovoltaic models using Lambert W-function collaborated with AI-based Puma optimization method*, *Results in Engineering* 25, 2025.

2. American Council on Renewable Energy (ACORE). *The Role of Renewable Energy in National Security*. Issue Brief, October 2018.
3. Assareh E., Keykhah A., Bedakhanian A., N. Agarwal, M. Lee*, Optimizing solar photovoltaic farm-based cogeneration systems with artificial intelligence (AI) and Cascade compressed air energy storage for stable power generation and peak shaving: A Japan-focused case study*, Applied Energy 377, 2025.
4. Brinkley J., Jiang L., Widyolar B., Hota., S.K., Bhusal Y., Diaz G., Winston R., *Thermal, electrical, and cost study of advanced optical photovoltaic thermal system (ADOPTS)*, Applied Energy 269, 2020.
5. IEA Photovoltaic Power Systems Programme (IEA-PVPS). *Snapshot of Global PV Markets 2023*. Report IEA-PVPS T1-42:2024, April 2024.
6. International Energy Agency (IEA). *Energy Security*. [Online]. Dostęp: IEA Topics – Energy Security, 2025.
7. International Renewable Energy Agency (IRENA). *Geopolitics of the Energy Transformation: Energy Security*, 2023.
8. International Energy Agency (IEA). *Solar PV – Analysis and Forecasts 2023*. IEA, 2024.
9. International Energy Agency (IEA). *The Role of Critical Minerals in Clean Energy Transitions*. Paryż: IEA, 2021.
10. International Energy Agency (IEA). *World Energy Outlook 2022*. Paryż: IEA, 2022.
11. Katir H., Abouloifa A., Lachkar I., Noussi K., Giri F., Guerrero J.M., *Advanced Nonlinear Control of A Grid-Connected Photovoltaic Power System Using N-Cascaded H-Bridge Multilevel Inverters*, IFAC PapersOnLine 53-2, 2020.
12. Khan K., Khurshid A., Cifuentes-Faura J., Xianjun D., *Does renewable energy development enhance energy security?* Utilities Policy, vol. 87, 2024.
13. Lamnatou Ch., Cristofari C., Chemisana D., *Artificial Intelligence (AI) in relation to environmental life-cycle assessment, photovoltaics, smart grids and small-island economies*, Sustainable Energy Technologies and Assessments 71, 2024.
14. Masterson V., *Here's how solar energy saved Europeans $29 billion this summer*, World Economic Forum, 2022.
15. National Renewable Energy Laboratory (NREL). *Resilient Solar Photovoltaics*. [Online]. NREL Security & Resilience. 2024.
16. Pandey A.K., Tyagi V.V., Selvaraj J., Rahim N.A., Tyagi S.K., *Recent advances in solar photovoltaic systems for emerging trends and advanced applications*, Renewable and Sustainable Energy Reviews 53, 2016.
17. *Panele fotowoltaiczne potencjalną furtką dla cyberprzestępców? Energetyka24.com*, 2021.
18. Papathanasiou D., *Why energy storage matters for the global energy transition*, World Bank Blogs, 2023.
19. REN21. *Renewables 2023 Global Status Report*. Paryż: REN21 Secretariat, 2023.
20. Sanchez J.H., Castro L.M., *Advanced three-stage photovoltaic system phasor model for grid integration dynamic studies*, Solar Energy 235, 2022.
21. Shaw V., Bellini E., *Longi achieves 34.6% efficiency for two-terminal tandem perovskite solar cell prototype*, PV Magazine International, 2024.

22. Togun H., Basem A., Jweeg M.J., Biswas N., Abed A.M., Paul D., Mohammed H.I., Chattopadhyay A., Sharma B.K., Abdulrazzaq T., *Advancing organic photovoltaic cells for a sustainable future: The role of artificial intelligence (AI) and deep learning (DL) in enhancing performance and innovation*, Solar Energy 291, 2025.
23. Tsuchida S., Nonaka H., Yamada N., *Deep Reinforcement Learning for the Optimal Angle Control of Tracking Bifacial Photovoltaic Systems*, Energies 15, 2022.
24. U.S. Department of Energy (DOE). *Sustainable and Holistic Integration of Energy Storage and Solar PV (SHINES)*. 2016.

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.

dr inż. Marta Chodyka
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0002-8819-2451
https://doi.org/10.29316/9788368103199_10

BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH A FUNKCJONOWANIE PRZEDSIĘBIORSTW W POLSCE

CYBERSECURITY OF INFORMATION SYSTEMS AND ITS IMPACT ON BUSINESS OPERATIONS IN POLAND

Streszczenie

W dobie intensywnej cyfryzacji bezpieczeństwo systemów informatycznych stanowi fundament sprawnego funkcjonowania współczesnych przedsiębiorstw. Rozdział podejmuje problematykę wpływu poziomu cyberbezpieczeństwa na działalność firm w Polsce, koncentrując się na analizie danych za rok 2024. Celem badania było określenie, w jakim stopniu inwestycje w bezpieczeństwo IT przekładają się na ciągłość działania, wyniki ekonomiczne i odporność organizacyjną. Zastosowano metodę mieszaną – analizę danych wtórnych (raporty CERT Polska, GUS, KPMG) oraz studia przypadków rzeczywistych incydentów (ransomware, wycieki danych, ataki łańcuchowe). Pytanie badawcze dotyczyło zależności między poziomem zabezpieczeń a zakłóceniami działalności operacyjnej.

Summary

In the era of widespread digitalization, information systems security has become a cornerstone of effective business operations. This chapter addresses the impact of cybersecurity maturity on the functioning of enterprises in Poland, focusing on data from 2024. The objective of the study was to assess how investments in IT security influence operational continuity, financial performance, and organizational resilience. A mixed-method approach was applied, combining secondary data analysis (reports from CERT Polska, GUS, KPMG) with case studies of real incidents (ransomware, data breaches, supply-chain attacks). The research question explored the relationship between cybersecurity readiness and operational disruptions. Findings indicate that

Wyniki wskazują, że rosnąca liczba incydentów oraz ich złożoność stanowią realne zagrożenie, szczególnie dla sektorów finansowego i handlu. Rozdział potwierdza, że systemowe podejście do cyberbezpieczeństwa stanowi kluczowy element strategii zarządzania ryzykiem i warunek stabilności przedsiębiorstw.

Słowa kluczowe: analiza ryzyka, ataki hakerskie, cyberbezpieczeństwo, ochrona danych, systemy informatyczne

the increasing frequency and complexity of incidents pose a tangible threat, especially to the financial and retail sectors. The chapter confirms that a systemic approach to cybersecurity is a critical component of risk management strategies and a prerequisite for business stability.

Keywords: cyberattacks, cybersecurity, data protection, information systems, risk analysis

Wstęp

W dobie intensywnej cyfryzacji procesów biznesowych oraz dynamicznie rozwijających się technologii informacyjnych zagadnienie bezpieczeństwa systemów informatycznych nabiera kluczowego znaczenia dla funkcjonowania współczesnych przedsiębiorstw. Wraz z rosnącą liczbą zagrożeń cybernetycznych oraz ich złożonością, kwestia zapewnienia wysokiego poziomu cyberbezpieczeństwa staje się integralnym elementem strategii zarządzania ryzykiem operacyjnym oraz warunkiem koniecznym stabilności biznesowej.

Niniejsza praca podejmuje problem wpływu poziomu zabezpieczeń systemów informatycznych na działalność przedsiębiorstw działających na terenie Polski. Przedmiotem badania jest analiza zależności pomiędzy dojrzałością organizacyjną w zakresie cyberbezpieczeństwa a zdolnością przedsiębiorstw do zapewnienia ciągłości działania, osiągania założonych wyników ekonomicznych oraz realizacji strategii rozwoju w obliczu realnych zagrożeń. Zdefiniowano następujące pytanie badawcze: W jakim stopniu poziom cyberbezpieczeństwa determinuje stabilność operacyjną i odporność organizacyjną polskich przedsiębiorstw na cyberzagrożenia? Hipotezą badawczą pracy jest założenie, że wysoki poziom zabezpieczeń informatycznych bezpośrednio przekłada się na stabilność operacyjną oraz ogranicza negatywne skutki incydentów cybernetycznych, podczas gdy niedostateczne zabezpieczenia skutkują poważnymi zakłóceniami operacyjnymi i stratami finansowymi oraz wizerunkowymi. W realizacji celów badawczych wykorzystano metodę mieszaną, obejmującą zarówno analizę danych wtórnych, jak i studia przypadków. Na etapie wstępnym przeprowadzono przegląd literatury przedmiotu, standardów międzynarodowych (głównie norm serii ISO/IEC 27000) oraz dobrych praktyk z zakresu cyberbezpieczeństwa, co umożliwiło sformułowanie podstawowych

definicji oraz ram teoretycznych pracy. Kolejnym etapem było przeprowadzenie analizy danych ilościowych pochodzących z raportów takich instytucji, jak Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający w Polsce, Główny Urząd Statystyczny oraz międzynarodowa firma doradcza KPMG, które opisują aktualny stan bezpieczeństwa informatycznego w polskich przedsiębiorstwach w roku 2024. Ostatnim elementem analizy było przygotowanie szczegółowych studiów przypadków, które ilustrują realne scenariusze incydentów bezpieczeństwa w Polsce. Wybrano trzy reprezentatywne przykłady różniące się charakterem zagrożeń (atak *ransomware*, wyciek danych osobowych oraz atak typu *supply-chain*), aby możliwie kompleksowo przedstawić spektrum konsekwencji operacyjnych, finansowych, prawnych oraz reputacyjnych.

Wyniki przeprowadzonych badań wskazują na istotne znaczenie systemowego podejścia do bezpieczeństwa informatycznego. Udowodniono, że organizacje dysponujące dobrze rozwiniętą infrastrukturą zabezpieczeń oraz procedurami ciągłości działania potrafią znacznie szybciej identyfikować zagrożenia, skutecznie je neutralizować oraz minimalizować skutki incydentów. Natomiast przedsiębiorstwa, które zaniedbały ten aspekt działalności, doświadczają poważnych, często długofalowych konsekwencji operacyjnych, finansowych i reputacyjnych. Praca potwierdza więc, że proaktywne inwestowanie w cyberbezpieczeństwo nie powinno być postrzegane jako opcjonalny koszt, lecz strategiczna inwestycja zapewniająca długoterminową stabilność biznesową.

Cyberbezpieczeństwo w zarządzaniu organizacjami – standardy, zagrożenia i dobre praktyki

Bezpieczeństwo systemów informatycznych (ang. *Information Systems Security*), często określane także jako cyberbezpieczeństwo, oznacza ochronę zasobów informacyjnych oraz teleinformatycznych organizacji przed zagrożeniami mogącymi naruszyć ich poufność, integralność oraz dostępność, co opisuje tzw. model CIA (ang. *Confidentiality, Integrity, Availability*)[1]. Klasyczne podejście oparte na tych trzech filarach często bywa rozszerzane o dodatkowe komponenty, takie jak identyfikacja i uwierzytelnianie użytkowników, kontrola dostępu, zapewnienie niezaprzeczalności działań oraz ochrona integralności

[1] J. Andress, Foundations of Information Securit, 2019.

i poufności transmisji danych[2]. Kompleksowe podejście do bezpieczeństwa obejmuje zarówno rozwiązania techniczne (np. szyfrowanie, zapory sieciowe, systemy wykrywania włamań, kopie zapasowe), jak i procedury organizacyjne (polityki bezpieczeństwa, szkolenia pracowników, zarządzanie ryzykiem). Celem jest stworzenie środowiska, w którym zasoby informacyjne są skutecznie chronione przed całym spektrum zagrożeń – od przypadkowych awarii po celowe ataki *hakerskie*.

W dobie powszechnej cyfryzacji działalności gospodarczej przedsiębiorstwa coraz bardziej uzależniają swoją efektywność operacyjną od niezawodnego działania systemów informatycznych. Transformacja cyfrowa przynosi wymierne korzyści biznesowe, ale jednocześnie zwiększa liczbę wektorów ataków wykorzystywanych przez cyberprzestępców. Zagrożenia cybernetyczne stanowią istotne wyzwanie dla organizacji ze wszystkich sektorów gospodarki – od finansowego, poprzez handel i przemysł, aż po infrastrukturę krytyczną. Incydenty takie jak, ataki typu *ransomware*, które paraliżują operacje, naruszenia danych osobowych skutkujące sankcjami regulacyjnymi, czy włamania do wewnętrznych sieci przedsiębiorstw, mogą powodować zakłócenia ciągłości działania, utratę zaufania interesariuszy oraz znaczne straty finansowe. W kontekście dynamicznie rosnącej liczby incydentów, odporność systemów informatycznych staje się nieodzownym elementem zarządzania ryzykiem operacyjnym. Elementy te wspólnie składają się na kompleksowe podejście do bezpieczeństwa systemów. Kompleksowe ujęcie bezpieczeństwa wymaga zatem zarówno rozwiązań technicznych (np. szyfrowanie, zapory sieciowe, systemy wykrywania włamań, kopie zapasowe), jak i procedur organizacyjnych (polityki bezpieczeństwa, szkolenia pracowników, zarządzanie ryzykiem). Celem jest stworzenie środowiska, w którym zasoby informacyjne przedsiębiorstwa są odpowiednio chronione przed całym spektrum zagrożeń – od przypadkowych awarii po celowe ataki hakerskie. Ważnym punktem odniesienia są tu międzynarodowe standardy, przede wszystkim ISO/IEC 27001[3] definiująca wymagania dla systemów zarządzania bezpieczeństwem informacji

[2] L. Chacko, P. Rajan, V. Anilkumar, V. Pathari, V., *Proof-of-Variable-Authority: A Blockchain Consensus Mechanism for Securing IoT Networks*, red. V. Muthukkumarasamy, S.D. Sudarsan, R.K. Shyamasundar, *Information Systems Security*, ICISS 2023, Lecture Notes in Computer Science, vol 14424. Springer, Cham, 2023.

[3] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, International Organization for Standardization, Geneva, 2022.

ISMS (ang. *Information Security Management System*). Zgodnie z normą ISO 27001 bezpieczeństwo informacji to zachowanie poufności, integralności i dostępności informacji, a także – w razie potrzeby – ich autentyczności, rozliczalności, niezawodności i przejrzystości. Standard ten, wraz z uzupełniającą normą ISO/IEC 27002[4] (zalecenia dot. zabezpieczeń) oraz powiązanymi normami (dotyczącymi ciągłości działania – ISO 22301[5], zarządzania ryzykiem – ISO 27005[6], bezpieczeństwa usług w chmurze – ISO 27017[7] i inne.), stanowi uznany zbiór dobrych praktyk. Coraz więcej polskich firm wdraża i certyfikuje systemy zarządzania bezpieczeństwem wg ISO 27001, choć nadal świadomość i dojrzałość w tym zakresie są zróżnicowane. Zgodność z międzynarodowymi standardami, takimi jak ISO/IEC 27001, ISO/IEC 27002, NIST *Cybersecurity Framework* czy powiązane normy sektorowe, pozwala organizacjom nie tylko ustrukturyzować działania ochronne, lecz także wykazać zgodność z obowiązującymi regulacjami prawnymi i branżowymi. W literaturze przedmiotu podkreśla się, że inwestycje w bezpieczeństwo informacji powinny być traktowane analogicznie do wydatków na ubezpieczenie – mogą wydawać się kosztowne, dopóki nie wystąpi incydent[8]. Ekonomiczne podejście do bezpieczeństwa informacji znajduje odzwierciedlenie w modelach optymalizacyjnych, które wskazują, że racjonalne jest inwestowanie w zabezpieczenia do poziomu, w którym marginalne ryzyko strat zrówna się z marginalnym kosztem ochrony. Oprócz teoretycznych ujęć, istotne są także dane empiryczne, m.in. coroczne raporty instytutów badawczych, które analizują finansowe skutki incydentów naruszenia danych. Zgodnie z raportem IBM *Security, Ponemon Institute*[9], średni globalny koszt pojedynczego incydentu naruszenia danych osiągnął rekordowy poziom 4,45 mln USD, co stanowi wzrost o 2,3% w porównaniu z rokiem poprzednim oraz o 15,3% od 2020 roku. Wskaźniki efektywności

[4] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*, International Organization for Standardization, Geneva, 2022.

[5] ISO 22301:2019, *Security and resilience — Business continuity management systems — Requirements*, International Organization for Standardization, Geneva, 2019.

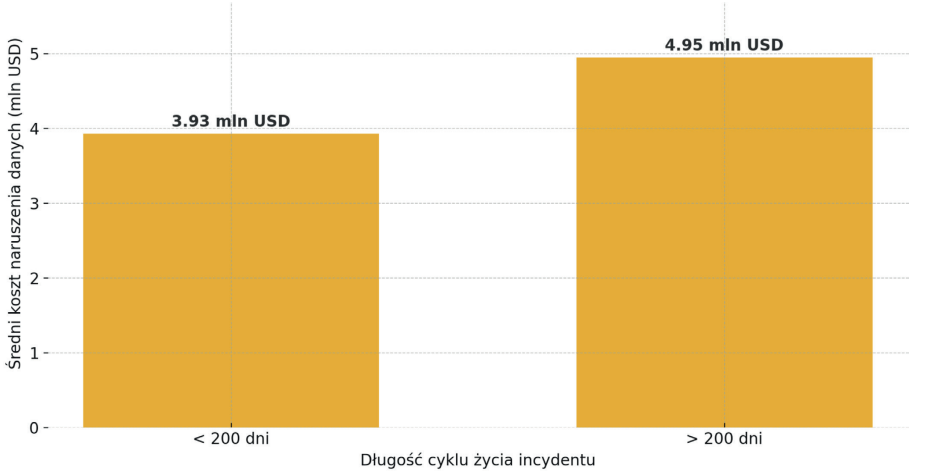
[6] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, International Organization for Standardization, Geneva, 2022.

[7] ISO/IEC 27017:2015, *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*, International Organization for Standardization, Geneva, 2015.

[8] L.A. Gordon, M.P. Loeb, M.P., *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, McGraw-Hill, 2006.

[9] IBM Security, Ponemon Institute, *Cost of a Data Breach Report,* 2023.

wykrywania pozostają niepokojące: organizacje potrzebują średnio 204 dni na identyfikację incydentu i kolejnych 73 dni na jego opanowanie, co łącznie daje 277 dni. Analiza wykazuje, że incydenty o cyklu życia krótszym niż 200 dni generowały średni koszt 3,93 mln USD, podczas gdy te trwające dłużej kosztowały średnio 4,95 mln USD, co oznacza wzrost o 1,02 mln USD. Rysunek 1 ilustruje zależność między długością cyklu życia incydentu a jego średnim kosztem, co pokazuje, że dłuższy czas identyfikacji i opanowania incydentu (powyżej 200 dni) wiąże się z wyraźnie wyższymi kosztami naruszeń danych – aż o 1,02 mln USD więcej w porównaniu z incydentami wykrytymi i opanowanymi szybciej. Szybsza identyfikacja i reakcja na incydenty są zatem kluczowe dla minimalizacji kosztów związanych z naruszeniami danych.



Rysunek 1. Zależność między długością cyklu życia incydentu a jego średnim kosztem
Źródło: opracowanie własne na podstawie danych IBM Security.

Statystyki te jasno obrazują, że szybka detekcja oraz natychmiastowa reakcja są kluczowe dla ograniczenia strat organizacyjnych. Niestety, wiele organizacji boryka się z ograniczeniami kadrowymi oraz niskim poziomem dojrzałości monitoringu. Według badania KPMG[10], ponad połowa firm wskazuje trudności z rekrutacją oraz utrzymaniem specjalistów z zakresu cyberbezpieczeństwa jako istotną barierę we wzmacnianiu swoich systemów ochronnych. Główne źródła zagrożeń nadal wiążą się z czynnikiem ludzkim – ataki

[10] KPMG, *Barometr Cyberbezpieczeństwa. Na fali czy w labiryncie regulacji?* – raport z badania ankietowego polskich przedsiębiorstw, KPMG Polska, 2024.

socjotechniczne, w szczególności *phishing*, pozostają najczęstszą formą inicjowania incydentów. Jak potwierdzają dane KPMG, kradzież danych osobowych i dostępów za pomocą *phishingu* jest nadal postrzegana jako najpoważniejsze zagrożenie cybernetyczne. Jednocześnie wzrasta liczba ataków typu *ransomware* – w 2022 r. ich częstotliwość globalnie wzrosła o około 13%, utrzymując się na poziomie uznawanym za kluczowe zagrożenie dla ciągłości działania firm[11]. Coraz powszechniejsze staje się stosowanie zaawansowanych technik inżynierii społecznej – m.in. rozmów telefonicznych lub wiadomości od przestępców podszywających się pod kadrę zarządzającą[12].

W ostatnich latach obserwuje się rosnącą świadomość organizacji w zakresie konieczności inwestowania w zaawansowane systemy ochrony zasobów informacyjnych. Coraz częściej wdrażane są rozwiązania wykorzystujące sztuczną inteligencję AI (ang. *Artificial Intelligence*) do wykrywania zagrożeń w czasie rzeczywistym, co pozwala na szybszą reakcję i ograniczenie skutków incydentów bezpieczeństwa. Pomimo tej tendencji, wdrażanie skutecznych systemów bezpieczeństwa nadal napotyka istotne bariery – w szczególności ograniczenia finansowe, niedobór wykwalifikowanych specjalistów z zakresu cyberbezpieczeństwa oraz złożoność przepisów prawnych i regulacyjnych. Na politykę bezpieczeństwa organizacji coraz większy wpływ mają regulacje normatywne na poziomie krajowym i unijnym. Do najważniejszych z nich należy dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej (tzw. dyrektywa NIS 2)[13] oraz ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2023 poz. 913)[14]. Ich celem jest podniesienie poziomu odporności państw członkowskich i operatorów usług kluczowych na zagrożenia cyfrowe poprzez ujednolicenie minimalnych standardów ochrony oraz obowiązków w zakresie raportowania incydentów. Zgodnie z wynikami badania przeprowadzonego przez KPMG, 45% przedsiębiorstw w Polsce deklaruje gotowość do

[11] Grant Thornton, *Cybersecurity report*, 2023.

[12] R. Chesney, D.K. Citron, D.K., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review*, 107(6), 2019, s. 1753-1820.

[13] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej (Dz. Urz. UE L 333 z 27.12.2022, s. 80).

[14] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2023 poz. 913).

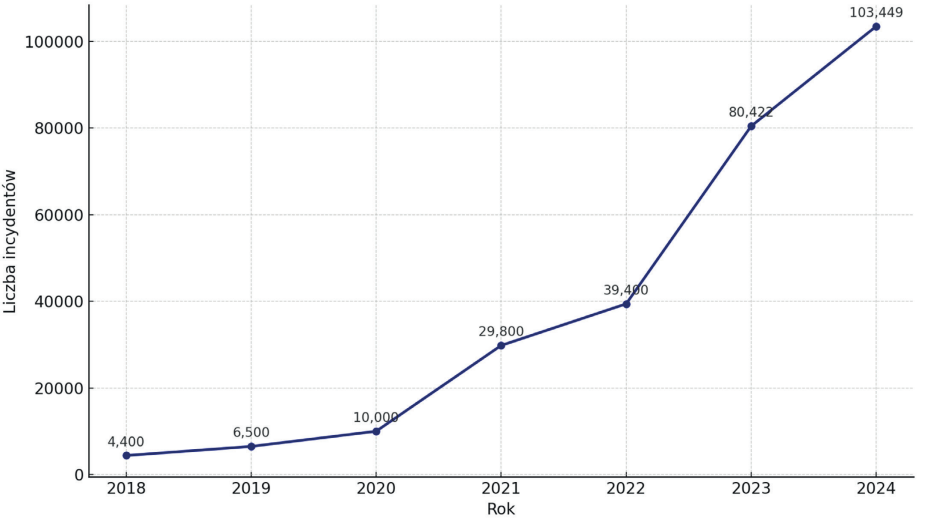
wdrożenia nowych przepisów[15]. Jednocześnie znacząca część organizacji zgłasza trudności w interpretacji obowiązków prawnych, co utrudnia skuteczne ich wdrażanie i może prowadzić do ryzyka regulacyjnego. Obowiązki takie jak konieczność zgłaszania incydentów do właściwego zespołu reagowania na incydenty bezpieczeństwa komputerowego CSIRT (ang. *Computer Security Incident Response Team*) [4] czy obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, stanowią silny impuls do doskonalenia praktyk zarządzania bezpieczeństwem informacji. Zarówno literatura naukowa, jak i dane empiryczne wskazują jednoznacznie, że cyberbezpieczeństwo nie powinno być traktowane jako opcjonalne narzędzie ochronne, lecz jako nieodzowny element zapewnienia ciągłości działania oraz utrzymania zaufania interesariuszy.

Dane wskazują, że zagrożenia cybernetyczne są zarówno powszechne, jak i bardzo zróżnicowane – obejmują ataki socjotechniczne, złośliwe oprogramowanie, a także zaawansowane, długotrwałe kampanie realizowane przez grupy APT (ang. *Advanced Persistent Threat*), charakteryzujące się wysokim stopniem ukierunkowania i trudnością w wykryciu. Ważne jest, że ataki te dotyczą nie tylko dużych organizacji, ale również małych i średnich przedsiębiorstw, które często dysponują ograniczonymi zasobami umożliwiającymi skuteczną reakcję. Nawet pozornie drobny incydent może więc prowadzić do poważnych konsekwencji operacyjnych, finansowych i wizerunkowych. W związku z tym odporność systemów informatycznych powinna być postrzegana nie tylko w aspekcie technologicznym, lecz także jako wynik synergii rozwiązań technicznych, kompetencji kadry zarządzającej, procedur reagowania oraz organizacyjnej gotowości na sytuacje kryzysowe. Kluczowe jest wdrożenie całościowego podejścia opartego na zarządzaniu ryzykiem, obejmującego zarówno identyfikację zagrożeń, jak i ocenę ich wpływu na krytyczne procesy biznesowe. W tym kontekście zapewnienie wysokiego poziomu cyberbezpieczeństwa nie może być traktowane jako opcjonalne, lecz stanowi kluczowy warunek zapewnienia ciągłości działania organizacji.

[15] KPMG, Barometr Cyberbezpieczeństwa. Na fali czy w labiryncie regulacji? – raport z badania ankietowego polskich przedsiębiorstw, KPMG Polska, 2024.

Stan cyberbezpieczeństwa w polskich przedsiębiorstwach

Dane empiryczne zebrane na podstawie raportów dotyczących incydentów cyberbezpieczeństwa jednoznacznie potwierdzają narastającą intensyfikację zagrożeń występujących w polskiej cyberprzestrzeni. Według raportu CERT Polska[16], krajowego zespołu reagowania na incydenty bezpieczeństwa CSIRT w 2024 roku liczba odnotowanych incydentów wyniosła aż 103 449, co oznacza wzrost o około 29% względem roku poprzedniego, kiedy to liczba zgłoszeń przekroczyła 80 tys.[17] Szczególnie wymowny jest wzrost liczby incydentów w perspektywie długookresowej – pięć lat wcześniej, czyli w roku 2019, odnotowano ich zaledwie 6,5 tysiąca. Oznacza to niemal dziesięciokrotną dynamikę wzrostową, co obrazuje zarówno realny wzrost liczby ataków, jak i poprawę skuteczności procedur ich wykrywania oraz raportowania przez przedsiębiorstwa i instytucje. Tendencję tę w ujęciu chronologicznym ilustruje rysunek 2.



Rysunek 2. Liczba incydentów cyberbezpieczeństwa w Polsce w latach 2018–2024
Źródło: opracowanie własne na podstawie danych CERT Polska.

[16] CERT Polska, *Raport roczny 2024. Incydenty naruszające bezpieczeństwo teleinformatyczne obsługiwane przez zespół CERT Polska,* NASK PIB, 2025.

[17] CERT Polska, *Raport roczny 2023. Incydenty naruszające bezpieczeństwo teleinformatyczne obsługiwane przez zespół CERT Polska*, NASK PIB, 2024.

Wzrost liczby incydentów cybernetycznych jest bezpośrednio powiązany z ewolucją ich charakteru oraz rosnącym zaawansowaniem technicznym. Według raportu CERT Polska (2024), dominującą kategorią zgłoszonych incydentów były oszustwa komputerowe, których udział sięgnął aż 94,7% wszystkich przypadków. Wśród nich szczególnie często pojawiał się *phishing* – metoda manipulacji społecznej polegająca na podszywaniu się cyberprzestępców pod zaufane podmioty w celu wyłudzenia informacji poufnych (np. loginów, haseł, danych bankowych). W 2024 roku *phishing* był najczęściej realizowany poprzez masowe kampanie mailowe oraz fałszywe strony internetowe, podszywające się między innymi pod znane serwisy sprzedażowe (OLX – ok. 10 tys. przypadków, Allegro – ok. 4 tys.) oraz społecznościowe (Facebook – prawie 4 tys. przypadków). Znacznie rzadziej zgłaszano szkodliwe oprogramowanie (ang. *malware*), które odpowiadało za 1,8% przypadków (1891 incydentów), czy wykorzystanie podatności usług informatycznych (1,6%, 1634 przypadków). Pozostałe kategorie, takie jak publikacja treści nielegalnych, włamania, zakłócenia dostępności usług, próby włamań, ataki na bezpieczeństwo informacji oraz nieautoryzowane gromadzenie danych, łącznie stanowiły mniej niż 2% zgłoszeń. Szczegółowe zestawienie struktury incydentów według kategorii przedstawiono w tabeli 1.

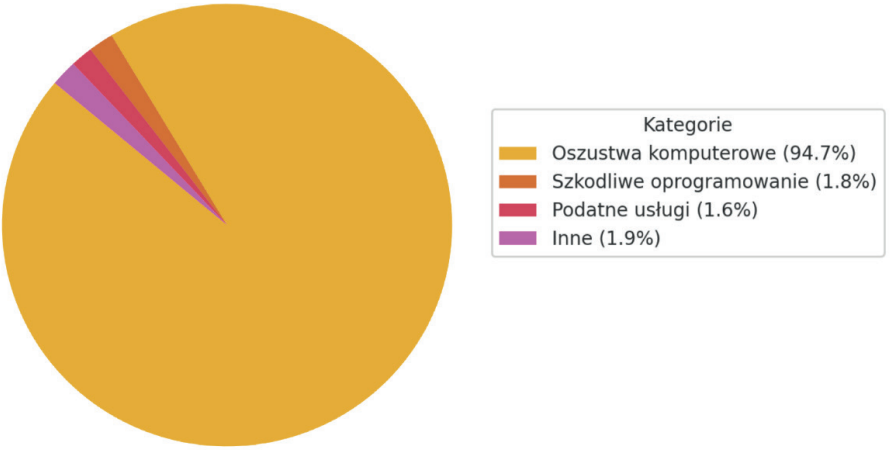
Tabela 1. Zestawienie incydentów cyberbezpieczeństwa według kategorii w Polsce za 2024 rok

Kategoria zagrożenia	Liczba incydentów	Udział procentowy
Oszustwa komputerowe	97 995	94,7%
Szkodliwe oprogramowanie	1 891	1,8%
Podatne usługi	1 634	1,6%
Obraźliwe i nielegalne treści	775	0,7%
Włamania	447	0,4%
Dostępność zasobów	426	0,4%
Próby włamań	179	0,2%
Atak na bezpieczeństwo informacji	62	0,1%
Gromadzenie informacji	26	0,0%
Inne	14	0,0%
Łącznie	103 449	100%

Źródło: opracowanie własne na podstawie danych CERT Polska.

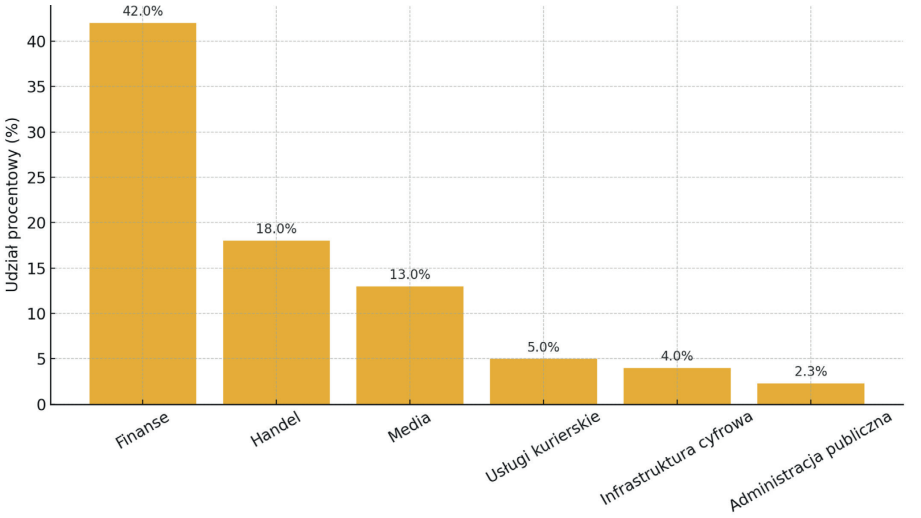
Szczegółową strukturę zgłoszonych incydentów przedstawiono na rysunku 3. Dominującą kategorią były oszustwa komputerowe, które odpowiadały za niemal 95% wszystkich zgłoszeń. Pozostałe kategorie, choć liczbowo

mniej liczne, wskazują na zróżnicowany charakter zagrożeń – od szkodliwego oprogramowania, przez nielegalne treści, po techniczne próby włamań i naruszenia dostępności usług. Dla zwiększenia czytelności, kategorie o najmniejszym udziale procentowym zostały zaszeregowane pod wspólnym mianem „Inne".



Rysunek 3. Struktura incydentów według kategorii w Polsce (2024)
Źródło: opracowanie własne na podstawie danych CERT Polska.

Analiza sektorowa wskazuje, iż poszczególne branże różnią się znacznie pod względem podatności na incydenty. Najbardziej zagrożony pozostaje sektor finansowy, na który przypada aż 42% wszystkich zarejestrowanych przez CERT Polska incydentów w 2024 roku. Kolejne sektory o wysokiej podatności to handel (18%) oraz media (13%). Niższy, lecz nadal znaczący poziom zagrożenia odnotowano w sektorze usług kurierskich (5%), infrastrukturze cyfrowej, obejmującej usługi telekomunikacyjne i centra danych (około 4%) oraz administracji publicznej (około 2,3%). Zestawienie danych zostało zaprezentowane na rysunku 4.



Rysunek 4. Udział sektorów w incydentach cyberbezpieczeństwa
Źródło: opracowanie własne na podstawie danych CERT Polska.

Te różnice sektorowe wynikają głównie ze specyfiki przetwarzanych danych oraz regulacji, które narzucają wyższe standardy ochrony na przykład instytucjom finansowym, co z kolei skutkuje lepszym raportowaniem incydentów. Jednocześnie, pomimo intensyfikacji zagrożeń, przedsiębiorstwa w Polsce wykazują coraz wyższy poziom świadomości potrzeby zabezpieczenia swoich zasobów informacyjnych. Według danych Głównego Urzędu Statystycznego[18], 94,1% przedsiębiorstw stosuje co najmniej jeden środek ochronny z technologii informacyjno-komunikacyjnych ICT (ang. *Information and Communication Technologies*). W przypadku dużych przedsiębiorstw wskaźnik ten jest jeszcze wyższy i sięga 99,6%. Najczęściej wdrażanymi zabezpieczeniami były: silne uwierzytelnianie (84% ogółu firm, 98,7% dużych), kontrola dostępu do sieci (64,5% ogółu firm, 97,9% dużych) oraz regularne kopie zapasowe w lokalizacjach zewnętrznych (71,4% ogółu, 96% dużych przedsiębiorstw). Niemniej jednak w ciągu ostatniego roku 32,5% firm doświadczyło przynajmniej jednego poważnego incydentu, z czego 10% wskazało na ponad 30 takich zdarzeń rocznie, co sugeruje konieczność dalszego doskonalenia systemów ochronnych. Najczęściej występowały incydenty techniczne związane

[18] GUS, *Społeczeństwo informacyjne w Polsce w 2024 roku.* Wyniki badań statystycznych z zakresu technologii informacyjno-komunikacyjnych w przedsiębiorstwach. Warszawa: Główny Urząd Statystyczny, 2024.

z awariami sprzętu i oprogramowania (29,7%), uszkodzeniem danych (7,7%) oraz ujawnieniem informacji poufnych w wyniku błędu ludzkiego (1%)[19].

Zgromadzone dane pozwalają stwierdzić, że rosnąca liczba incydentów oraz ich coraz bardziej zaawansowany charakter wymagają kompleksowego podejścia do zarządzania bezpieczeństwem, obejmującego techniczne, organizacyjne oraz edukacyjne aspekty ochrony danych. Szczególnego znaczenia nabiera wdrażanie strategii zapewnienia ciągłości działania BCP (ang. *Business Continuity Planning*) oraz strategii odzyskiwania danych po incydencie DRP (ang. *Disaster Recovery Planning*), jako kluczowych elementów budowania odporności organizacyjnej na cyberzagrożenia.

Analiza incydentów cyberbezpieczeństwa w polskich przedsiębiorstwach

Celem poniższej analizy jest zilustrowanie wpływu poziomu bezpieczeństwa systemów informatycznych na funkcjonowanie polskich przedsiębiorstw poprzez trzy szczegółowo zrekonstruowane studia przypadków incydentów cyberbezpieczeństwa. Wybrane przypadki dotyczą zróżnicowanych scenariuszy ataków – (1) *ransomware* na dużą firmę z branży gier wideo, (2) wycieku danych klientów popularnej platformy e-commerce oraz (3) ataku typu *supply-chain* wymierzonego w sektor finansowy. Każdy przypadek został opracowany na podstawie wiarygodnych źródeł (raportów incydentalnych, komunikatów firm, formalnych doniesień medialnych) i obejmuje opis przebiegu incydentu oraz analizę jego konsekwencji dla zaatakowanej organizacji w tym: zakłócenia operacyjne, straty finansowe, implikacje prawne, reputacyjne. Takie podejście pozwala ukazać szerokie spektrum zagrożeń cybernetycznych i ocenić, w jakim stopniu zaniedbania lub dobre praktyki w zakresie cyberbezpieczeństwa przekładają się na ciągłość działania przedsiębiorstw. Analiza tych przypadków stanowi podstawę do sformułowania wniosków na temat zależności między bezpieczeństwem systemów IT a kondycją biznesową firm oraz opracowania rekomendacji poprawy poziomu cyberbezpieczeństwa.

Przypadek 1: Atak ransomware na firmę z branży gier wideo (2021).
Na początku lutego 2021 roku doszło do jednego z najgłośniejszych cyberataków na polskie przedsiębiorstwo prywatne – ofiarą padła znana firma z branży gier wideo, producent popularnych tytułów. Atakujący włamali się

[19] CERT Polska, Raport roczny 2024. Incydenty naruszające bezpieczeństwo teleinformatyczne obsługiwane przez zespół CERT Polska, NASK PIB, 2025.

do wewnętrznej sieci tego przedsiębiorstwa i wdrożyli oprogramowanie *ransomware*, szyfrując dane na serwerach. Napastnicy pozostawili notatkę z żądaniem okupu oraz groźbą ujawnienia wykradzionych informacji, twierdząc, że pozyskali m.in. kody źródłowe flagowych gier oraz poufne dokumenty korporacyjne (finansowe, kadrowe itp.). Firma stanęła przed trudnym wyborem: zapłacić okup (bez gwarancji odzyskania danych i uniknięcia publikacji wycieku) albo odmówić i zmierzyć się z konsekwencjami. Zarząd ostatecznie postanowił nie ulegać szantażowi – spółka publicznie potwierdziła incydent, zawiadomiła organy ścigania i kategorycznie odmówiła zapłaty. W odpowiedzi sprawcy spełnili swoje groźby: w kolejnych dniach w Internecie zaczęły pojawiać się fragmenty skradzionych kodów źródłowych gier oraz firmowej dokumentacji, udostępniane na podziemnych forach i prawdopodobnie oferowane do sprzedaży na czarnym rynku. Skutki tego incydentu okazały się poważne i wielowymiarowe dla zaatakowanej spółki. Po pierwsze, zakłócenia operacyjne: znaczna część wewnętrznych systemów IT została zaszyfrowana lub prewencyjnie wyłączona. Między innymi infrastruktura deweloperska służąca do tworzenia oprogramowania przestała być dostępna, co wymusiło przerwanie prac projektowych. Firma musiała opóźnić publikację raportu finansowego za rok 2020 z powodu paraliżu wywołanego atakiem. Po drugie, straty finansowe i rynkowe: w dniu upublicznienia informacji o ataku kurs akcji spółki spadł na giełdzie o ok. 4%, a niepewność co do skali wycieku oraz potencjalnych dalszych konsekwencji dodatkowo obciążyła reputację firmy – już nadwątloną wcześniejszymi problemami z jednym z flagowych produktów. Choć nie podano dokładnych kwot strat, sam przestój operacyjny i koszty naprawy infrastruktury IT szacowano na wielomilionowe sumy. Po trzecie, implikacje prawne: wśród ujawnionych danych znalazły się m.in. dane personalne pracowników (np. dokumenty HR), co stwarzało ryzyko naruszenia przepisów o ochronie danych osobowych i zainteresowało Urząd Ochrony Danych Osobowych. Dodatkowo, jeśli w wykradzionej poufnej korespondencji wewnętrznej ujawniłyby się ewentualne zaniedbania zarządu, spółce mogły grozić pozwy od akcjonariuszy. Po czwarte, szkody wizerunkowe: paradoksalnie atak ten pokazał, że nawet firma technologiczna – od której oczekuje się najwyższych standardów w IT – miała luki w zabezpieczeniach. Publiczna dyskusja wokół incydentu wskazywała, że reputacja przedsiębiorstwa ucierpiała, a zaufanie inwestorów i partnerów biznesowych zostało naruszone. Analiza tego przypadku prowadzi do kilku ważnych obserwacji. Po pierwsze, atak *ransomware* uderza nie tylko w finansowe aspekty działalności, ale i strategiczne

– w tym wypadku napastnicy zaatakowali najbardziej wartościowe zasoby intelektualne firmy (kody źródłowe gier stanowiące jej kluczową własność intelektualną). Po drugie, odporność organizacji i plany awaryjne są kluczowe. W opisywanym przedsiębiorstwie posiadanie aktualnych kopii zapasowych oraz dobrze opracowanych procedur ciągłości działania pozwoliło stosunkowo szybko przywrócić podstawowe operacje, mimo zaszyfrowania części systemów – raportowano, że kluczowe funkcje udało się odzyskać w ciągu kilkunastu dni. Niemniej jednak sam fakt skutecznego włamania obnażył braki w prewencji, prawdopodobnie zawiódł któryś z mechanizmów ochronnych (np. atak rozpoczął się od skutecznego *phishingu* dającego dostęp do sieci albo brak segmentacji sieci pozwolił *malware* na szerokie rozprzestrzenienie). Po trzecie, incydent posłużył jako sygnał ostrzegawczy dla innych firm w Polsce – nawet rynkowi liderzy nie są w pełni bezpieczni. W branży *gamingowej* po tym wydarzeniu wiele podmiotów przeprowadziło dodatkowe audyty zabezpieczeń, testy penetracyjne oraz wdrożyło bardziej restrykcyjne polityki (typu *zero trust*) w celu zapobieżenia podobnym incydentom w przyszłości.

Przypadek 2: Wyciek danych klientów platformy e-commerce (2018-2019).

Drugie *case study* dotyczy poważnego incydentu, który dotknął jedną z czołowych polskich platform e-commerce działających w branży sprzedaży elektroniki. Pod koniec 2018 roku cyberprzestępcom udało się włamać do bazy danych klientów tego sklepu internetowego, co doprowadziło do wycieku informacji o ponad 2,2 miliona użytkowników. Skradzione dane obejmowały między innymi imiona i nazwiska klientów, adresy e-mail, numery telefonów, adresy dostawy, a także hasła (zaszyfrowane, lecz potencjalnie podatne na złamanie) oraz historię zakupów. Ujawnienie tak szerokiego zakresu danych osobowych – w tym danych kontaktowych i pośrednio preferencji zakupowych – stanowiło jeden z największych incydentów naruszenia ochrony danych w polskim e-commerce. Konsekwencje dla przedsiębiorstwa okazały się bardzo poważne i długofalowe. Bezpośrednio po wykryciu wycieku (w grudniu 2018 r.) firma musiała zmierzyć się z kryzysem wizerunkowym oraz obowiązkiem prawym powiadomienia zarówno klientów, jak i właściwego organu nadzorczego o zaistniałym incydencie. Uruchomiono procedury informowania wszystkich poszkodowanych osób (co samo w sobie stanowiło ogromne wyzwanie logistyczne przy tak dużej liczbie rekordów), a także wsparcia dla klientów – m.in. zalecono pilną zmianę haseł we wszystkich usługach, ostrzegano przed próbami *phishingu* wykorzystującymi wykradzione dane itd. Reakcja organu

nadzorczego była zdecydowana: w 2019 roku Prezes Urzędu Ochrony Danych Osobowych nałożył na spółkę administracyjną karę pieniężną w wysokości 2,8 mln zł za niewystarczające zabezpieczenie danych osobowych klientów. Była to wówczas rekordowo wysoka kara w Polsce za naruszenie przepisów RODO. W uzasadnieniu decyzji Urzędu Ochrony Danych Osobowych UODO wskazano m.in. brak stosowania dwuskładnikowego uwierzytelniania 2FA (ang. *Two-Factor Authentication*) w kluczowych procesach bezpieczeństwa – na przykład podczas logowania administratorów do systemu informatycznego lub klientów do swoich kont. Dwuskładnikowe uwierzytelnianie polega na konieczności potwierdzenia tożsamości użytkownika za pomocą dwóch niezależnych elementów (np. hasła oraz jednorazowego kodu SMS lub aplikacji mobilnej). Zaniedbanie tego mechanizmu znacząco ułatwiło atakującym przejęcie dostępu do chronionych danych[20]. Spółka odwołała się od decyzji, jednak w 2020 r. Wojewódzki Sąd Administracyjny podtrzymał nałożenie kary, a następnie w 2021 r. organ nadzorczy, odkrywszy dodatkowe obciążające okoliczności, zwiększył wymiar grzywny do 3,8 mln zł. Tak dotkliwa sankcja finansowa znacząco obciążyła wyniki firmy za dany okres i stała się wyraźnym sygnałem ostrzegawczym dla całej branży, że zaniedbania w ochronie danych klientów będą surowo karane. Oprócz konsekwencji prawnych, firma poniosła także poważne straty reputacyjne. Wielu klientów utraciło zaufanie do platformy – tym bardziej, że sprawa była szeroko komentowana w mediach, a w Internecie szybko pojawiły się bazy wyciekłych danych (narażając osoby na spam oraz kolejne ataki socjotechniczne). Konkurenci nie wahali się wykorzystać sytuacji w przekazach marketingowych, podkreślając bezpieczeństwo swoich rozwiązań. Szacuje się, że w wyniku skandalu część użytkowników przeniosła się z tej platformy do innych serwisów, a wskaźniki sprzedaży sklepu przejściowo spadły. Firma, chcąc odzyskać reputację, musiała zainwestować w kampanię odbudowy zaufania – wzmocniono obsługę klienta, oferowano poszkodowanym m.in. darmowy monitoring tożsamości oraz rabaty na kolejne zakupy. Wewnętrznie incydent stał się impulsem do gruntownego przeglądu zabezpieczeń: wprowadzono obowiązkową weryfikację dwuskładnikową 2FA dla klientów i administratorów systemu, zatrudniono dodatkowych specjalistów ds. bezpieczeństwa IT, wdrożono system DLP (ang. *Data Loss Prevention*), czyli rozwiązanie zapobiegające nieautoryzowanemu wyciekowi danych

[20] UODO – Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 2019 r. w sprawie naruszenia ochrony danych osobowych w sklepie Morele.net (publikacja na stronie UODO.gov.pl) ZSPR.421.2.2019, 2019.

poza organizację, a także zaostrzono polityki dostępu do informacji uznawanych za krytyczne z punktu widzenia bezpieczeństwa operacyjnego. Systemy DLP umożliwiają monitorowanie, wykrywanie i blokowanie prób przesyłania wrażliwych danych poprzez różne kanały komunikacji (np. e-mail, nośniki USB, chmurę), minimalizując ryzyko ich niekontrolowanego ujawnienia. Głośnym echem odbił się przy tym fakt, iż atakujący najprawdopodobniej uzyskali wstępny dostęp do systemu, wysyłając do firmy zainfekowany dokument CV (życiorys) i wykorzystując podatność w oprogramowaniu pocztowym – co unaoczniło znaczenie edukacji pracowników oraz stosowania filtrów bezpieczeństwa nawet w tak rutynowych procesach, jak rekrutacja. Podsumowując, ten przypadek pokazuje, że wyciek danych osobowych klientów przekłada się na bardzo realne straty finansowe (kary administracyjne, koszty naprawy), operacyjne (czasochłonna obsługa incydentu, dodatkowe procedury) i wizerunkowe, które mogą obciążać firmę przez długi czas. Stanowi on również przestrogę, iż spełnianie jedynie minimalnych wymogów prawnych to za mało – przedsiębiorstwa muszą proaktywnie rozwijać swoje systemy zabezpieczeń i wdrażać najlepsze praktyki (choćby tak podstawowe jak dwuskładnikowe uwierzytelnianie), zanim to poważny incydent wymusi takie działania.

Przypadek 3: Atak *supply-chain* poprzez stronę regulatora finansowego (2016-2017).

Trzeci przypadek ilustruje zaawansowany incydent cyberbezpieczeństwa klasyfikowany jako atak łańcucha dostaw (ang. *supply-chain attack*), który dotknął polski sektor bankowy na przełomie lat 2016 i 2017. Incydent ten został uznany za bezprecedensowy w skali kraju ze względu na nietypowy wektor ataku oraz fakt, że jego źródłem była instytucja nadzoru finansowego. Zamiast dokonywać bezpośrednich prób naruszenia systemów bankowych, sprawcy uzyskali dostęp do infrastruktury teleinformatycznej Komisji Nadzoru Finansowego (KNF) – centralnego organu regulacyjnego rynku finansowego w Polsce. W wyniku kompromitacji serwera instytucji, napastnicy zmodyfikowali zawartość oficjalnej strony internetowej KNF, wprowadzając do niej złośliwy kod. W efekcie, w okresie od października 2016 roku do lutego 2017 roku, użytkownicy odwiedzający witrynę – w tym pracownicy instytucji finansowych – byli narażeni na automatyczne pobranie zewnętrznego pliku zawierającego złośliwe oprogramowanie (ang. *malware*). Wykorzystanie infrastruktury zaufanego podmiotu nadzorczego jako wektora ataku umożliwiło rozprzestrzenienie się zagrożenia na szereg banków komercyjnych. Dopiero w styczniu 2017 roku kilka instytucji finansowych niemal

równocześnie zaobserwowało anomalie w ruchu sieciowym oraz nieznane pliki na serwerach, których nie wykrywały stosowane dotąd rozwiązania antywirusowe. Analiza przeprowadzona przez zespoły bezpieczeństwa działające w ramach sektorowego zespołu reagowania (CSIRT KNF oraz jednostka przy Związku Banków Polskich) pozwoliła na identyfikację wspólnego mianownika – wszystkie zainfekowane stacje robocze wcześniej komunikowały się z witryną KNF. 3 lutego 2017 roku, w ramach działań zaradczych, infrastruktura informatyczna Komisji Nadzoru Finansowego została prewencyjnie wyłączona, celem przerwania ciągu infekcji oraz zabezpieczenia materiału dowodowego. Śledztwo wykazało, że incydent umożliwił napastnikom uzyskanie potencjalnie głębokiego dostępu do wewnętrznych segmentów sieci bankowych, co mogło pozwolić na dalsze działania z zakresu rekonesansu, eskalacji uprawnień lub wycieku danych. Zgodnie z oficjalnymi informacjami, incydent nie doprowadził do kradzieży danych klientów ani środków finansowych. Istnieją jednak przesłanki wskazujące, że celem ataku było cyberszpiegostwo, tj. pozyskanie informacji oraz przygotowanie gruntu pod potencjalne dalsze operacje cybernetyczne. Incydent ten uwypuklił słabość zaufanych relacji instytucjonalnych – nawet podmioty pełniące funkcje regulacyjne i nadzorcze mogą, wskutek luk w zabezpieczeniach, stać się punktem wejścia dla cyberzagrożeń. W oficjalnym komentarzu opublikowanym przez Rządowe Centrum Bezpieczeństwa (RCB), podkreślono, że podstawowym błędem było założenie, iż serwis informacyjny instytucji nie wymaga szczególnej ochrony – założenie to zostało bezwzględnie wykorzystane przez atakujących. Incydent unaocznił również kluczowe znaczenie współpracy międzyinstytucjonalnej w zakresie cyberbezpieczeństwa. Dzięki szybkiej wymianie informacji pomiędzy zespołami reagowania banków, CSIRT KNF oraz zespołami CSIRT NASK i Agencji Bezpieczeństwa Wewnętrznego, możliwe było szybkie zidentyfikowanie źródła ataku i ograniczenie jego skutków. Gdyby każda instytucja działała w izolacji, wykrycie wektora infekcji mogłoby zająć znacznie więcej czasu, zwiększając potencjalne straty. Konsekwencje tego incydentu były znaczące zarówno z perspektywy reputacyjnej, jak i operacyjnej. Komisja Nadzoru Finansowego zmuszona była do odbudowy zaufania oraz modernizacji swoich systemów, natomiast banki przeprowadziły kosztowne działania naprawcze i audyty bezpieczeństwa. W odpowiedzi na ten atak sektor finansowy zaostrzył procedury bezpieczeństwa, wprowadzając m.in. kontrolę kanałów zaufanych, audyty aplikacji dostarczanych przez podmioty trzecie oraz ćwiczenia typu „*red teaming*", symulujące podobne scenariusze zagrożeń. Atak ten stanowi

dziś klasyczny przykład incydentu łańcucha dostaw i jest często omawiany w kontekście szkoleń i konferencji branżowych. Pokazuje on, że bezpieczeństwo cyfrowe całego ekosystemu zależy od najsłabszego ogniwa – niezależnie od formalnej roli danej instytucji w strukturze rynku.

Zaprezentowane powyżej trzy studia przypadków – obejmujące atak typu *ransomware*, incydent związany z wyciekiem danych osobowych oraz atak typu łańcucha dostaw (ang. *supply-chain attack*) – obrazują złożoność oraz zróżnicowanie zagrożeń cybernetycznych, na jakie narażone są współczesne organizacje. Przypadki te uwidaczniają szerokie spektrum możliwych skutków incydentów bezpieczeństwa – od bezpośrednich strat finansowych i zakłóceń operacyjnych, poprzez konsekwencje prawne i regulacyjne, aż po długofalową utratę reputacji i zaufania interesariuszy. Analiza tych zdarzeń potwierdza tezę, że niedostateczny poziom zabezpieczeń – w tym brak mechanizmów redundancji danych (np. regularnych kopii zapasowych), brak wdrożenia mechanizmów silnego uwierzytelniania (np. dwuskładnikowego uwierzytelniania, czy też utrzymywanie nieaktualnego oprogramowania – znacząco zwiększa prawdopodobieństwo wystąpienia skutecznych ataków oraz pogłębia ich negatywne konsekwencje. Z drugiej strony, organizacje wykazujące wysoki poziom dojrzałości w zakresie zarządzania bezpieczeństwem informacji – posiadające zaktualizowane plany ciągłości działania, skuteczne strategie odzyskiwania po awarii, regularne kopie zapasowe oraz wewnętrzną kulturę bezpieczeństwa opartą na świadomości i kompetencjach pracowników – są zdecydowanie lepiej przygotowane na sytuacje kryzysowe. Tego rodzaju podejście umożliwia im szybsze przywrócenie funkcjonowania po incydencie oraz ograniczenie strat, zarówno materialnych, jak i niematerialnych. Z perspektywy zarządzania ryzykiem operacyjnym, studia przypadków te stanowią istotny materiał analityczny, wskazując, że inwestycje w cyberbezpieczeństwo należy traktować nie jako koszt, lecz jako element nieodzowny dla utrzymania odporności organizacyjnej w warunkach gospodarki cyfrowej.

Wnioski i rekomendacje dla podniesienia poziomu bezpieczeństwa

Przeprowadzone analizy potwierdzają istotną zależność: poziom bezpieczeństwa systemów informatycznych znacząco wpływa na ciągłość działania i wyniki przedsiębiorstw. Innymi słowy, hipoteza badawcza mówiąca, iż wysoki poziom cyberbezpieczeństwa jest kluczowym czynnikiem warunkującym stabilność operacyjną firm, została pozytywnie zweryfikowana. Widzimy

wyraźnie, że firmy inwestujące w zabezpieczenia IT (technologie, procedury, kadry) nie tylko zmniejszają prawdopodobieństwo wystąpienia incydentu, ale także lepiej radzą sobie w razie ataku – szybciej wykrywają zagrożenie, skuteczniej ograniczają jego rozprzestrzenianie i sprawniej przywracają normalne operacje. Z kolei zaniedbania w bezpieczeństwie prowadzą do poważnych zakłóceń działalności: atak *ransomware* może sparaliżować podstawowe procesy na wiele dni, wyciek danych klientów skutkuje kosztownymi karami oraz utratą zaufania, a atak na infrastrukturę informatyczną może przerwać ciągłość kluczowych usług. W skrajnym przypadku następstwem poważnego cyberataku bywa nawet upadłość przedsiębiorstwa – literatura odnotowuje przykłady, gdzie kumulacja kosztów i utraty reputacji po incydencie doprowadziła organizacje do bankructwa. Warto podkreślić, że koszty incydentów cyberbezpieczeństwa są bardzo wysokie. Średni globalny koszt naruszenia danych wynosi obecnie około 4,45 mln USD, a średni koszt incydentu *ransomware* sięga 5,23 mln USD[21]. Równie kosztowny bywa długi czas reakcji – firmy, które szybko wykrywają i neutralizują zagrożenie, ponoszą istotnie mniejsze straty niż te, u których atak pozostaje niezauważony przez wiele miesięcy. Niestety, jak wspomniano wcześniej, wykrycie ataku zajmuje organizacjom średnio ponad pół roku. Jakie działania powinny zatem podjąć polskie przedsiębiorstwa, aby zminimalizować ryzyko wystąpienia incydentów i złagodzić ich skutki? Poniżej przedstawiono kluczowe rekomendacje wynikające z dokonanej analizy przypadków oraz aktualnych dobrych praktyk:

- Implementacja wielowarstwowych zabezpieczeń (ang. *defence-in-depth*): Należy wdrażać wiele niezależnych mechanizmów ochronnych na różnych poziomach. Podstawą są aktualne systemy antywirusowe i zapory sieciowe, ale równie ważne jest szyfrowanie wrażliwych danych, segmentacja sieci (utrudniająca rozprzestrzenianie się złośliwego oprogramowania) oraz systemy wykrywania włamań IDS/IPS (ang. *Intrusion Detection System* / *Intrusion Prevention System*). Konieczne jest stosowanie silnego uwierzytelniania – co najmniej dwuskładnikowego (2FA) – wszędzie tam, gdzie to możliwe, zarówno dla dostępu pracowników do systemów wewnętrznych, jak i dla użytkowników usług online. Przykład

[21] IBM Security, Ponemon Institute, Cost of a Data Breach Report, 2023.

kary nałożonej przez UODO na platformę e-commerce[22] pokazuje, że brak 2FA może zostać uznany za poważne zaniedbanie.

- Regularne kopie zapasowe i plany ciągłości działania: Ataki *ransomware* oraz inne awarie wymuszają posiadanie aktualnych kopii zapasowych kluczowych danych, przechowywanych w odseparowanej infrastrukturze (zgodnie z zasadą 3-2-1: trzy kopie na dwóch różnych nośnikach, w tym jedna kopia *off-site*). Firmy powinny okresowo testować odtwarzanie systemów z backupów, by upewnić się, że kopie są skuteczne. Ponadto każdy przedsiębiorca powinien dysponować Planem Ciągłości Działania (BCP) oraz Planem Odzyskiwania po Awarii (DRP), które precyzują procedury funkcjonowania w trybie awaryjnym, dopuszczalne czasy przestoju dla krytycznych procesów oraz role i odpowiedzialności zespołów w razie poważnego incydentu. W opisanym przypadku firmy z sektora gier posiadanie sprawnych backupów pozwoliło odtworzyć systemy po ataku w akceptowalnym czasie, ograniczając długość przestoju – takie plany muszą jednak być regularnie aktualizowane i ćwiczone (np. poprzez symulacyjne testy typu *table-top*).
- Monitorowanie i szybka detekcja zagrożeń: Biorąc pod uwagę długi medianowy czas wykrywania incydentów (ponad 200 dni globalnie), przedsiębiorstwa muszą zainwestować w zaawansowane narzędzia monitoringu bezpieczeństwa. Nowoczesne systemy klasy SIEM (ang. *Security Information and Event Management*) oraz SOAR (ang. *Security Orchestration, Automation and Response*), umożliwiające zaawansowaną analizę, automatyzację i skuteczne reagowanie na incydenty bezpieczeństwa. Systemy te potrafią agregować logi z różnych źródeł i automatyzować detekcję anomalii, a dedykowane zespoły SOC (ang. *Security Operations Center*) lub usługi zarządzanego monitoringu zapewniają całodobowy nadzór nad bezpieczeństwem. Warto korzystać z mechanizmów *threat intelligence* – bieżących informacji o pojawiających się zagrożeniach – aby móc szybko reagować na nowe kampanie ataków (np. CERT Polska udostępnia listy ostrzeżeń o aktywnych *phishingach*). Współczesne rozwiązania wykorzystujące uczenie maszynowe mogą znacząco skrócić czas wykrycia subtelnych ataków. Długotrwałe niewykrycie incydentu, jak pokazał przypadek ataku na KNF trwającego kilka miesięcy w tle,

[22] UODO – Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 2019 r. w sprawie naruszenia ochrony danych osobowych w sklepie Morele.net (publikacja na stronie UODO.gov.pl) ZSPR.421.2.2019, 2019.

pozwala napastnikom zadomowić się w sieci ofiary i zwiększa potencjalne szkody. Dlatego celem każdej firmy powinno być maksymalne zredukowanie czasu bytności atakującego w systemie (ang. *dwell time)* – np. poprzez stosowanie agentów EDR (ang. *Endpoint Detection and Response*) / XDR (ang. *Extended Detection and Response*) na stacjach roboczych, które wychwytują podejrzane aktywności (takie jak nieautoryzowana eskalacja uprawnień czy komunikacja z nietypowymi domenami).

- Szkolenia i podnoszenie świadomości pracowników: Czynnik ludzki jest jednym z najsłabszych ogniw bezpieczeństwa, którego nie da się w pełni wyeliminować technologią, dlatego kluczowe jest zbudowanie w organizacji silnej kultury bezpieczeństwa. Regularne szkolenia personelu z rozpoznawania ataków socjotechnicznych (ang. *phishingu, vishingu* itp.), zasad higieny haseł, bezpiecznych praktyk pracy z systemami oraz procedur zgłaszania incydentów są absolutnie niezbędne. Szkolenia powinny mieć praktyczny charakter (np. okresowo przeprowadzane symulowane kampanie *phishingowe* testujące czujność załogi) i być dostosowane do specyfiki danej firmy. Świadomy zagrożeń pracownik może okazać się najskuteczniejszą linią obrony – na przykład to czujność pracowników banków pozwoliła zauważyć anomalie wskazujące na atak przez stronę KNF, co przyczyniło się do wykrycia opisanego incydentu. Warto promować zasadę *zero trust but verify* – nawet wewnątrz organizacji personel powinien weryfikować nietypowe polecenia lub prośby (np. dotyczące transferów środków), nawet jeśli pozornie pochodzą od kadry zarządzającej, gdyż zdarzają się oszustwa typu BEC (ang. *Business Email Compromise*).
- Audyt bezpieczeństwa dostawców i partnerów (ang. *security of supply chain*): Firmy powinny oceniać ryzyka związane z podmiotami zewnętrznymi, które mają dostęp do ich systemów lub danych. Opisany atak *supply-chain* na sektor bankowy dobitnie pokazał, że słabo zabezpieczony partner (w tym wypadku strona WWW organu nadzoru) może zagrozić wielu niezależnym organizacjom. W praktyce należy uwzględniać wymagania bezpieczeństwa już na etapie zawierania umów z dostawcami – wprowadzać klauzule dotyczące standardów zabezpieczeń, prawa do audytu bezpieczeństwa, obowiązku zgłaszania incydentów itp. Dobrą praktyką jest okresowe sprawdzanie kluczowych partnerów pod kątem przestrzegania podstawowych zasad cyberbezpieczeństwa (czy regularnie aktualizują

oprogramowanie, czy nie doświadczyli ostatnio incydentu, który mógłby rozprzestrzenić się na infrastrukturę firmy). Należy również technicznie ograniczać zaufanie do dostawców: segmentować i minimalizować zakres dostępu partnerów zewnętrznych tylko do zasobów niezbędnych do realizacji usług (zasada najmniejszych uprawnień). Szczególnie wrażliwe integracje (np. połączenia z systemami regulatorów czy banków) powinny być objęte dodatkowym monitoringiem i dodatkowymi warstwami zabezpieczeń.

- Zgodność z regulacjami i standardami: Przedsiębiorstwa – zwłaszcza z sektorów kluczowych (finanse, energetyka, transport, zdrowie) – muszą spełniać wymogi krajowe i unijne w zakresie cyberbezpieczeństwa. Nowa unijna dyrektywa w sprawie bezpieczeństwa sieci i informacji NIS2 (ang. *Network and Information Security Directive*)[23], nałoży w najbliższym czasie jeszcze szersze obowiązki na tzw. podmioty istotne. Do najważniejszych z nich należą m.in. konieczność wdrożenia adekwatnych środków technicznych i organizacyjnych dostosowanych do poziomu ryzyka oraz obowiązek zgłaszania poważnych incydentów bezpieczeństwa w ciągu 24 godzin od ich wykrycia. Choć dyrektywa jest już wiążąca dla państw członkowskich UE, w Polsce nie została jeszcze formalnie implementowana do krajowego porządku prawnego. Obecnie trwają prace legislacyjne nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa – projekt ten znajduje się na etapie konsultacji międzyresortowych. Zakończenie procesu legislacyjnego i wejście w życie odpowiednich przepisów spodziewane jest w pierwszej połowie 2025 roku. Już teraz jednak warto przygotować się do nadchodzących wymogów, przeprowadzając analizę luk (tzw. *gap analysis*) względem przyszłych regulacji NIS2 i uzupełniając brakujące elementy – takie jak polityki i procedury bezpieczeństwa, mechanizmy zarządzania ryzykiem, czy ustalone kanały współpracy z zespołami reagowania na incydenty (CSIRT). Podobnie wymogi RODO dotyczące ochrony danych osobowych muszą być traktowane priorytetowo – przypadek wycieku danych i rekordowej kary dla omawianej platformy e-commerce dowodzi, że *compliance* przekłada się na konkretne koszty (lepiej zawczasu zainwestować w zabezpieczenia niż później płacić wysokie kary). Dobrą praktyką podnoszącą

[23] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej, znana jako dyrektywa NIS2, 2022.

poziom zaufania jest również uzyskanie certyfikacji zgodności z normą ISO/IEC 27001 – choć formalnie nieobowiązkowa, certyfikacja taka potwierdza dojrzałość systemu zarządzania bezpieczeństwem informacji w firmie i bywa wymagana przez niektórych kontrahentów (zwłaszcza międzynarodowych).

- Plan reagowania na incydenty oraz współpraca w ramach ekosystemu: Każda organizacja powinna posiadać sformalizowany plan reagowania na incydenty IRT (ang. *Incident Response Plan*), określający skład i role zespołu reagowania, procedury eskalacji problemu, zasady komunikacji (zarówno wewnętrznej, jak i z mediami oraz klientami) oraz współpracy z organami ścigania i odpowiednimi CSIRT-ami. Przećwiczenie potencjalnych scenariuszy (np. symulacja ataku *ransomware* w formie *war game*) pozwala uniknąć chaosu w sytuacji prawdziwego kryzysu. Bardzo istotna jest także współpraca sektorowa i udział w inicjatywach wymiany informacji o zagrożeniach (np. sieci ISAC w różnych sektorach). Przykład banków pokazuje, że dzielenie się wiedzą o zaobserwowanym ataku umożliwiło sprawne wykrycie jego źródła i ograniczenie skutków. Budowanie zaufanych kanałów współpracy (np. grupy robocze pod auspicjami Związku Banków Polskich, fora wymiany informacji między operatorami infrastruktury krytycznej itp.) zwiększa wspólną odporność całego ekosystemu na ataki. W przypadku mniejszych firm, które nie dysponują rozbudowanymi zespołami IT, warto rozważyć współpracę z wyspecjalizowanymi podmiotami zewnętrznymi (firmami doradczymi, integratorami bezpieczeństwa), aby w razie incydentu móc szybko uzyskać ekspercką pomoc. Uzupełnieniem strategii zarządzania ryzykiem może być także wykupienie ubezpieczenia cyberryzyk – polisa co prawda nie zapobiegnie atakowi, ale może częściowo złagodzić jego skutki finansowe (trzeba przy tym pamiętać, że warunkiem wypłaty odszkodowania jest zwykle posiadanie podstawowych zabezpieczeń, co stanowi dodatkową motywację do ich wdrożenia).

Reasumując, cyberbezpieczeństwo stało się nieodłącznym elementem zarządzania nowoczesnym przedsiębiorstwem. Wyniki powyższych analiz jednoznacznie wskazują, że wysoki poziom zabezpieczeń warunkuje stabilność i zrównoważony rozwój firm w cyfrowej gospodarce. Nakłady na bezpieczeństwo informacji należy traktować jak inwestycję chroniącą przed potencjalnie druzgocącymi stratami. Przedsiębiorstwa działające w Polsce powinny systematycznie podnosić poziom dojrzałości w zakresie cyberbezpieczeństwa,

obejmując działania zarówno w obszarze technologii, jak i procesów organizacyjnych oraz zasobów ludzkich. Tylko kompleksowe, proaktywne podejście do zarządzania bezpieczeństwem informacji, oparte na współpracy wszystkich uczestników ekosystemu, pozwala skutecznie minimalizować negatywne skutki incydentów bezpieczeństwa dla działalności operacyjnej organizacji. W kontekście rosnącej skali i złożoności zagrożeń, konieczne jest nie tylko wdrażanie odpowiednich narzędzi technicznych, lecz również budowanie świadomości i kompetencji wśród pracowników oraz zapewnienie gotowości decyzyjnej i operacyjnej w sytuacjach kryzysowych.

Podsumowanie

W rozdziale przeanalizowano związek pomiędzy poziomem bezpieczeństwa systemów informatycznych a funkcjonowaniem przedsiębiorstw w warunkach rosnących zagrożeń cybernetycznych. Wykorzystując podejście mieszane – łączące analizę danych empirycznych z krajowych raportów oraz studia przypadków realnych incydentów – wykazano, że dojrzałość organizacyjna w zakresie cyberbezpieczeństwa jest jednym z kluczowych determinantów ciągłości działania, stabilności finansowej i odporności operacyjnej przedsiębiorstw.

Przeprowadzone badania potwierdziły, że brak odpowiednich zabezpieczeń technicznych, organizacyjnych oraz kompetencyjnych skutkuje poważnymi konsekwencjami – zarówno w wymiarze bezpośrednich strat finansowych i operacyjnych, jak i długofalowej utraty reputacji. Przypadki takie jak ataki ransomware, wycieki danych osobowych czy kompromitacje infrastruktury pośredników zaufania, jednoznacznie ukazują, że cyberzagrożenia nie są zjawiskiem marginalnym, lecz systemowym ryzykiem wymagającym skoordynowanej odpowiedzi. Z drugiej strony, przedsiębiorstwa charakteryzujące się wysokim poziomem dojrzałości w zakresie zarządzania bezpieczeństwem informacji – wdrażające standardy branżowe, realizujące polityki ciągłości działania, monitorujące infrastrukturę w czasie rzeczywistym oraz inwestujące w edukację pracowników – wykazują wyraźnie większą odporność na incydenty i szybciej odzyskują zdolność operacyjną po ich wystąpieniu.

Wnioski płynące z rozdziału wskazują, że cyberbezpieczeństwo powinno być postrzegane jako strategiczny obszar zarządzania ryzykiem, a nie kosztowny dodatek technologiczny. Wdrażanie rozwiązań zgodnych z normami międzynarodowymi (takimi jak ISO/IEC 27001), rozwój mechanizmów

monitorowania i reagowania (SIEM, SOAR, EDR/XDR), doskonalenie planów BCP i DRP oraz systematyczna edukacja kadry stanowią podstawę budowania odporności organizacyjnej. Rozdział stanowi zatem zarówno diagnozę obecnego stanu bezpieczeństwa informatycznego polskich przedsiębiorstw, jak i zbiór praktycznych wskazówek dla decydentów odpowiedzialnych za strategię bezpieczeństwa cyfrowego.

Literatura

1. Andress, J., *Foundations of Information Security: A Straightforward Introduction*, 2nd ed., No Starch Press, San Francisco, 2019.
2. Chacko, L., Rajan, P., Anilkumar, V., Pathari, V. *Proof-of-Variable-Authority: A Blockchain Consensus Mechanism for Securing IoT Networks*, [w:] *Information Systems Security*, ed. V. Muthukkumarasamy, S. D. Sudarsan, R. K. Shyamasundar, ICISS 2023, Lecture Notes in Computer Science, vol. 14424, Springer, Cham, 2023.
3. Chesney, R., Citron, D.K. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, California Law Review, 107(6), 2019, s. 1753-1820.
4. Gordon, L.A., Loeb, M.P. Managing Cybersecurity Resources: A Cost-Benefit Analysis, McGraw-Hill, 2006.
5. CERT Polska, Raport roczny 2023. Incydenty naruszające bezpieczeństwo teleinformatyczne obsługiwane przez zespół CERT Polska, NASK PIB, 2024.
6. CERT Polska, Raport roczny 2024. Incydenty naruszające bezpieczeństwo teleinformatyczne obsługiwane przez zespół CERT Polska, NASK PIB, 2025.
7. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej (Dz. Urz. UE L 333 z 27.12.2022, s. 80), 2022.
8. Grant Thornton, Cybersecurity Report, 2023.
9. GUS, Społeczeństwo informacyjne w Polsce w 2024 roku. Wyniki badań statystycznych z zakresu technologii informacyjno-komunikacyjnych w przedsiębiorstwach, Główny Urząd Statystyczny, Warszawa, 2024.
10. IBM Security, Ponemon Institute, Cost of a Data Breach Report, 2023.
11. International Organization for Standardization, ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements, Geneva, 2019.
12. International Organization for Standardization, ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Geneva, 2022.
13. International Organization for Standardization, ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls, Geneva, 2022.
14. International Organization for Standardization, ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks, Geneva, 2022.

15. International Organization for Standardization, ISO/IEC 27017:2015, Code of practice for information security controls based on ISO/IEC 27002 for cloud services, Geneva, 2015.
16. KPMG, Barometr Cyberbezpieczeństwa. Na fali czy w labiryncie regulacji? – raport z badania ankietowego polskich przedsiębiorstw, KPMG Polska, 2024.
17. UODO, Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 2019 r. w sprawie naruszenia ochrony danych osobowych w sklepie Morele.net, ZSPR.421.2.2019, publikacja na stronie UODO.gov.pl, 2019.
18. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, (Dz. U. 2023 poz. 913).

dr Mariusz Czternastek
Uniwersytet Komisji Edukacji Narodowej w Krakowie
ORCID: 0000-0002-0396-9904

dr Sławomir Żurawski
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0001-9527-3391

mgr Marek Chwała
Uniwersytet Komisji Edukacji Narodowej w Krakowie
ORCID: 0000-0003-3853-1897

mgr Patryk Ochyra
Menedżerska Akademia Nauk Stosowanych w Warszawie
ORCID: 0000-0001-8991-4068
https://doi.org/10.29316/9788368103199_11

PAŃSTWOWA STRAŻ POŻARNA JAKO ISTOTNY ELEMENT ZARZĄDZANIA KRYZYSOWEGO PODCZAS WYSTĄPIENIA POWODZI

THE STATE FIRE SERVICE AS AN IMPORTANT ELEMENT OF CRISIS MANAGEMENT DURING FLOODS

Streszczenie

Celem rozdziału jest analiza roli PSP jako realizatora zadań podczas powodzi. Pierwsza część rozdziału przedstawia znaczenie PSP w systemie zarządzania kryzysowego oraz opisuje podstawowe zadania tej służby

Summary

The aim of the chapter is to analyze the role of the State Fire Service in removing the effects of flooding. The first part of the chapter presents the importance of the State Fire Service in the crisis management system and

podczas powodzi. Druga część koncentruje się na sprzęcie i technologiach wykorzystywanych przez PSP w akcjach ratowniczych, podkreślając znaczenie nowoczesnych narzędzi i technologii. Ostatnia część analizuje konkretne przypadki działań PSP, w tym interwencje podczas powodzi na Śląsku w 2024 roku, wskazując na trudności, wyzwania i wnioski płynące z tych wydarzeń. Problem badawczy sformułowano: Jakie działania podejmuje Państwowa Straż Pożarna w czasie powodzi i w jaki sposób można zwiększyć skuteczność jej interwencji? W pracy zastosowano analizę literatury przedmiotu oraz raportów dotyczących zarządzania kryzysowego, przegląd aktów prawnych regulujących działania PSP, a także analizę studiów przypadków, w tym powodzi na Śląsku w 2024 roku. Działania PSP podczas powodzi są kluczowym elementem zarządzania kryzysowego, jednak dalszy rozwój technologii ratowniczych, usprawnienie koordynacji między służbami oraz inwestycje w szkolenia mogą znacząco zwiększyć skuteczność tych działań w przyszłości.

Słowa kluczowe: Państwowa Straż Pożarna, zarządzanie kryzysowe, powódź, działania ratownicze, nowoczesne technologie

describes the basic tasks of this service during floods. The second part focuses on the equipment and technologies used by the State Fire Service in rescue operations, emphasizing the importance of modern tools and technologies. The last part analyzes specific cases of PSP activities, including interventions during the flood in Silesia in 2024, pointing to the difficulties, challenges and conclusions from these events. The research problem was formulated: What actions does the State Fire Service take during floods and how can the effectiveness of its intervention be increased? The paper uses an analysis of scientific literature and reports on crisis management, a review of legal acts regulating the activities of the State Fire Service, as well as an analysis of case studies, including the flood in Silesia in 2024. The activities of the State Fire Service during floods are a key element of crisis management, but further development of rescue technologies, improved coordination between services and investments in training can significantly increase the effectiveness of these activities in the future.

Keywords: State Fire Service, crisis management, flood, rescue operations, modern technologies

Wstęp

Powódź jest jednym z najgroźniejszych i najbardziej niszczycielskich zjawisk naturalnych, które mogą wystąpić w wyniku intensywnych opadów deszczu, roztopów śniegu, niewłaściwego zarządzania wodami lub zmian klimatycznych. W krótkim czasie może ona zalać ogromne obszary, powodując straty materialne, zagrażając zdrowiu i życiu ludzi, a także niszcząc infrastrukturę krytyczną. Działania ratunkowe w czasie powodzi są niezwykle trudne i wymagają szybkiej reakcji, odpowiedniej organizacji oraz współpracy różnych służb, by skutecznie minimalizować straty i chronić obywateli. W tym kontekście, Straż Pożarna odgrywa nieocenioną rolę jako jedna z podstawowych służb ratunkowych.

Straż Pożarna jest często pierwszą instytucją, która wchodzi w teren zagrożony powodzią, podejmując działania mające na celu ratowanie osób uwięzionych w wodzie, ewakuację mieszkańców oraz zabezpieczanie mienia. Ponadto, strażacy zajmują się także likwidowaniem zagrożeń związanych z wodą, takich jak awarie infrastruktury wodociągowej, usuwanie zatorów wodnych, czy ochrona przed osunięciami ziemi. Dzięki specjalistycznemu wyposażeniu – takim jak łodzie ratunkowe, pompy do wypompowywania wody czy systemy monitorowania poziomu wód – Straż Pożarna jest w stanie podejmować skuteczne działania, nawet w najtrudniejszych warunkach.

Działania strażaków w czasie powodzi nie ograniczają się jednak tylko do interwencji w terenie. PSP jest także częścią szerokiego systemu zarządzania kryzysowego, współpracując z innymi służbami, takimi jak policja, wojsko, służby medyczne, władze samorządowe i organizacje pozarządowe. Koordynacja działań tych instytucji ma kluczowe znaczenie dla efektywności całego procesu ratunkowego, zwłaszcza w obliczu dynamicznie zmieniającej się sytuacji kryzysowej. Ponadto, strażacy są odpowiedzialni za prowadzenie działań prewencyjnych i edukacyjnych, które mają na celu zmniejszenie ryzyka powodziowego oraz przygotowanie społeczeństwa do możliwych zagrożeń.

Rozdział ma na celu identyfikację roli Państwowej Straży Pożarnej jako kluczowego elementu systemu zarządzania kryzysowego podczas powodzi. Zostaną omówione zarówno zadania, jakie strażacy realizują w takich sytuacjach, jak i wyzwania, przed którymi stają w trakcie akcji ratunkowych. Zostanie również zaprezentowana współpraca straży pożarnej z innymi służbami, jak również analiza konkretnych działań podejmowanych w przeszłości, które ukazują znaczenie tej służby w kontekście ochrony ludzkiego życia i mienia podczas katastrof powodziowych.

Działania Państwowej Straży Pożarnej – wybrane aspekty

Powódź jest jednym z najbardziej destrukcyjnych zjawisk naturalnych, które w Polsce występują coraz częściej, w wyniku zmieniających się warunków klimatycznych, intensyfikacji opadów deszczu oraz roztopów śnieżnych. Skala tego zagrożenia może prowadzić do poważnych uszkodzeń infrastruktury, utraty mienia oraz zagrożenia życia ludzkiego. W takich sytuacjach kluczową rolę w systemie zarządzania kryzysowego odgrywa Państwowa Straż Pożarna (PSP), jak również jest istotnym elementem systemu ochrony

przeciwpowodziowej w Polsce[1]. Z uwagi na swoje zadania, kompetencje i wyposażenie, PSP pełni rolę głównego organu odpowiedzialnego za akcje ratunkowe, prewencję oraz zarządzanie kryzysowe w czasie powodzi. Według ustawy o PSP do podstawowych zadań Państwowej Straży Pożarnej należy m.in.:

- rozpoznawanie zagrożeń pożarowych i innych miejscowych zagrożeń;
- organizowanie i prowadzenie akcji ratowniczych w czasie pożarów, klęsk żywiołowych lub likwidacji miejscowych zagrożeń;
- wykonywanie zadań ochrony ludności i obrony cywilnej;
- wykonywanie pomocniczych specjalistycznych czynności ratowniczych w czasie klęsk żywiołowych lub likwidacji miejscowych zagrożeń przez inne służby ratownicze[2].

PSP nie jest podmiotem zarządzania kryzysowego. Realizuje natomiast zadania wykonawcze na rzecz właściwych podmiotów (organów administracji publicznej)[3]. Podstawowym zadaniem Państwowej Straży Pożarnej w czasie powodzi jest zapewnienie bezpieczeństwa ludzkiego życia. To PSP jako pierwsza zostaje powiadomiona o zagrożeniu powodziowym, uruchamiając procedury ewakuacyjne i interwencyjne. Strażacy dysponują odpowiednim przeszkoleniem oraz specjalistycznym sprzętem, który umożliwia im skuteczną pomoc w trudnych warunkach. W sytuacji zagrożenia powodziowego zadaniem PSP jest zarówno przeprowadzanie ewakuacji ludności z terenów zagrożonych zalaniem, jak i ratowanie osób, które utknęły w zalanych budynkach czy na niebezpiecznych terenach. W przypadku osób, które zostały uwięzione w wyniku powodzi, PSP jest również odpowiedzialna za przeprowadzenie akcji ratunkowych, w tym transport do bezpiecznych miejsc.

PSP, w ramach swoich obowiązków, odpowiada także za zabezpieczenie mienia oraz kluczowej infrastruktury, której usunięcie mogłoby prowadzić do poważniejszych skutków powodziowych. W tym przypadku działania Straży Pożarnej obejmują m.in. zabezpieczanie obiektów użyteczności publicznej, ochronę zbiorników wodnych, wałów przeciwpowodziowych oraz systemów

[1] M. Misterka, *Analiza działań Państwowej Straży Pożarnej podczas powodzi w 2010 roku w świetle usprawniania ochrony przeciwpowodziowej w Polsce – część 1*, Zeszyty Naukowe SGSP, nr 56(4), 2015, s. 42.

[2] Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej Dz. U. 1991 Nr 88, poz. 400), art. 1, pkt 2.

[3] P. Gromek, *Państwowa Straż Pożarna a zarządzanie kryzysowe. Ujęcie strukturalne*, Zeszyty Naukowe SGSP, nr 63/3, 2017, s. 32.

kanalizacyjnych. Ponadto, PSP realizuje zadania związane z zapobieganiem uszkodzeniom infrastruktury energetycznej i gazowej, co może zminimalizować ryzyko kolejnych niebezpieczeństw, takich jak wybuchy gazu czy pożary.

Ważnym elementem działań PSP podczas powodzi jest usuwanie przeszkód w rzekach oraz innych zbiornikach wodnych, które mogą prowadzić do powstania dodatkowych zagrożeń. PSP wykonuje także prace mające na celu odblokowanie ścieków czy drenów, aby zapobiec powstawaniu nowych zatorów, które mogą skutkować powiększeniem się obszaru zalania. Straż Pożarna angażuje się również w organizowanie punktów pomocy medycznej, gdzie osoby poszkodowane w wyniku powodzi mogą liczyć na szybką pomoc. Strażacy są wyspecjalizowani w udzielaniu pierwszej pomocy medycznej w trudnych warunkach, co jest szczególnie istotne, ponieważ powódź często prowadzi do obrażeń i kontuzji.

Państwowa Straż Pożarna pełni również kluczową rolę w działaniach prewencyjnych, które mają na celu minimalizowanie ryzyka wystąpienia powodzi oraz ograniczanie jej skutków. Działania te są równie ważne, co interwencje ratunkowe, ponieważ ich celem jest nie tylko reagowanie na sytuacje kryzysowe, ale także zapobieganie im. PSP bierze aktywny udział w monitorowaniu stanu wód w rzekach i innych ciekach wodnych, a także nadzoruje stan wałów przeciwpowodziowych, zbiorników wodnych oraz kanałów i zapór. Straż pożarna współpracuje z Instytutem Meteorologii i Gospodarki Wodnej, przekazując informacje o zmianach w poziomie wód oraz prognozach hydrologicznych, co umożliwia szybsze podejmowanie decyzji o ewentualnych działaniach prewencyjnych. Przekaz informacji i prawidłowa ich analiza oraz ocena są niejako gwarantem skuteczności działania służb ratowniczych[4].

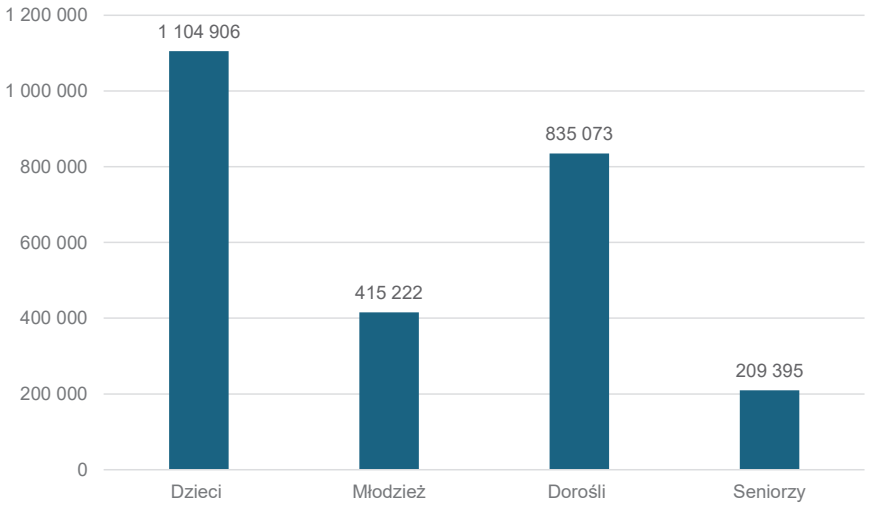
Doraźna struktura zarządzania kryzysowego w jednostce organizacyjnej PSP powinna realizować następujące, podstawowe zadania:

- potwierdzanie istoty, charakteru i zasięgu sytuacji kryzysowej lub kryzysu;
- przejmowanie kontroli nad sytuacją kryzysową lub kryzysem w drodze zaplanowanych działań;
- doprowadzenie do stanu, kiedy zagrożenia funkcjonowania jednostki organizacyjnej PSP nie rozwijają się;

[4] Z. Ciekanowski, S. Żurawski, *Państwowa Straż Pożarna jako grupa dyspozycyjna w systemie zarządzania kryzysowego*, Aviation and Security Issues, nr 1(1), 2022, s. 28.

- maksymalne ograniczenie skutków oddziaływania zagrożeń (np. wstępna odbudowa reputacji);
- komunikacja z interesariuszami (m.in. organami administracji publicznej, przedstawicielami innych służb, inspekcji i straży, dziennikarzami)[5].

PSP prowadzi także szeroką działalność edukacyjną i prewencyjną wśród ludności, organizując spotkania informacyjne, ćwiczenia i symulacje, w których mieszkańcy zagrożonych terenów uczą się zasad ewakuacji, udzielania pierwszej pomocy oraz reagowania w przypadku powodzi. Na poniższym rysunku przedstawiono liczbę przeszkolonej w 2024 roku populacji Polski z zakresu działań Prewencji Społecznej PSP.



Rysunek 1. Liczba przeszkolonej populacji Polski z zakresu działań Prewencji Społecznej PSP z podziałem na grupy wiekowe

Źródło: Podsumowanie działań prewencji społecznej, Komenda Główna Państwowej Straży Pożarnej.

Jak wynika z powyższego rysunku w 2024 roku Państwowa Straż Pożarna przeszkoliła 2 564 596 osób w ramach działań Prewencji Społecznej, co stanowi 6,8% populacji Polski. Dzięki takim działaniom możliwe jest zwiększenie świadomości społeczeństwa na temat zagrożeń powodziowych oraz przygotowanie go na szybszą reakcję w obliczu kryzysu. Prewencja ma na celu nie tylko zwiększenie odporności społeczeństwa na powódź, ale także zmniejszenie liczby ofiar oraz ograniczenie zniszczeń w wyniku katastrofy.

[5] *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*, red. R.W. Kaszubski, D. Romańczuk, Wydawnictwo FTB przy ZBP, Warszawa 2012.

Aby skutecznie reagować na powódź, PSP musi współpracować z szeregiem innych służb i instytucji, które są częścią systemu zarządzania kryzysowego. Takie skoordynowane działanie umożliwia szybsze podejmowanie decyzji, sprawniejszą organizację ewakuacji oraz efektywne wykorzystanie zasobów. W przypadku powodzi PSP współpracuje z jednostkami wojskowymi, które wspierają działania ratunkowe, szczególnie w przypadku, gdy dochodzi do zniszczenia infrastruktury komunikacyjnej. Straż Pożarna współdziała również z Policją, która zajmuje się organizowaniem transportu ewakuacyjnego i zabezpieczaniem terenów dotkniętych powodzią przed rabunkiem czy nielegalnym wtargnięciem osób trzecich. Dodatkowo, w czasie działań ratunkowych współpracuje ze Służbą Zdrowia, koordynując transport rannych i poszkodowanych do szpitali.

PSP współpracuje także z organizacjami pozarządowymi, które oferują pomoc w postaci zbiórek charytatywnych, transportu darów, organizacji schronisk dla ewakuowanych oraz pomocy psychologicznej dla poszkodowanych. Istnieje wiele fundacji pomocowych[6].

Dzięki współdziałaniu, pomoc dociera szybciej, a reakcja jest bardziej skoordynowana i skuteczna. Straż Pożarna współpracuje także z samorządami oraz administracją lokalną, co pozwala na dostosowanie działań do specyfiki regionu i szybkość reakcji na lokalne zagrożenia. W obliczu powodzi, PSP zmaga się z wieloma wyzwaniami, które wynikają z szybko zmieniającej się sytuacji. Intensyfikacja opadów deszczu, nieprzewidywalność kierunku przepływu wód oraz zmiany w strukturze terenu powodują, że strażacy muszą działać w warunkach dużej niepewności. Szybka reakcja jest niezbędna, aby uniknąć katastrofalnych skutków powodzi. Strażacy muszą być w pełni gotowi do podjęcia działań w różnych warunkach terenowych, w tym w obliczu trudnych warunków atmosferycznych, utrudnionego dostępu do poszkodowanych obszarów oraz braku wystarczających zasobów.

PSP musi być elastyczna i zdolna do dostosowania się do zmieniających się warunków, podejmując odpowiednie decyzje w zależności od sytuacji. Ponieważ prognozy meteorologiczne mogą się zmieniać, a poziom wód może rosnąć w sposób nieprzewidywalny, Straż Pożarna musi mieć gotowe scenariusze awaryjne oraz zasoby, które umożliwiają szybkie reagowanie w każdym momencie. Również w zakresie wykonywania działań podczas

[6] K. Zalewska, K. Ochyra-Żurawska, Z. Ciekanowski, *Organizacje pozarządowe w systemie bezpieczeństwa państwa*, Studia Administracji i Bezpieczeństwa, 13(13), 2022, s. 209.

akcji ratowniczej należy pamiętać, że zagrożenia takie jak powodzie oraz inne ryzyka naturalne, nie znają państwowych granic terytorialnych[7], dlatego współpraca wszystkich służb ratunkowych oraz koordynacja działań pozwala na efektywniejsze wykorzystanie dostępnych zasobów oraz skrócenie czasu reakcji.

Nie sposób pominąć roli, jaką w zakresie ochrony przeciwpowodziowej pełni Krajowy System Ratowniczo-Gaśniczy (KSRG). Jest to kluczowy element zapewniający bezpieczeństwo wewnętrzne kraju, a Państwowa Straż Pożarna została wyznaczona jako główny uczestnik tego systemu[8]. Państwowa Straż Pożarna pomimo dynamicznie zmieniających się warunków poszerza zakres swojej aktywności i działalności o działania specjalistyczne, lecz nadal istnieją podmioty ratownicze, które w sposób istotny mogą uzupełnić możliwości KSRG[9].

Wszystkie te elementy składają się na rolę Państwowej Straży Pożarnej w systemie zarządzania kryzysowego podczas powodzi. PSP nie tylko ratuje życie i zdrowie ludzkie, ale także skutecznie zabezpiecza mienie i infrastrukturę, zapewniając ochronę przed dalszymi zagrożeniami. Dzięki skutecznej współpracy z innymi służbami oraz instytucjami państwowymi i pozarządowymi, Straż Pożarna odgrywa kluczową rolę w zarządzaniu kryzysowym i minimalizowaniu skutków powodzi.

Sprzęt i technologie wykorzystywane przez Państwową Straż Pożarną w walce z powodziami

Państwowa Straż Pożarna (PSP) odgrywa kluczową rolę w systemie zarządzania kryzysowego, szczególnie podczas powodzi, które mogą stanowić poważne zagrożenie dla życia ludzkiego, mienia oraz infrastruktury. Działania PSP w czasie powodzi wymagają zastosowania zaawansowanego sprzętu i technologii, które umożliwiają szybką reakcję, skuteczne ratowanie ludzi, usuwanie wody oraz monitorowanie sytuacji kryzysowej. Współczesne

[7] J. Filaber, *Działania ratownicze ochotniczych straży pożarnych podczas akcji ratowniczych organizowanych i prowadzonych przez Państwową Straż Pożarną*, Acta Universitatis Wratislaviensis, no. 3861, 2018, s. 183.

[8] M. Misterka, *Analiza działań Państwowej* …, op. cit., s. 42.

[9] G. Pietrek, *Krajowy System Ratowniczo-Gaśniczy-zasadniczy element podsystemu wykonawczego zarządzania kryzysowego. Wnioski z powodzi 2010 rok*, [w:] *Systemy ratownicze w Polsce a bezpieczeństwo cywilne i wojskowe*, red. B. Zysiak-Christ, T. Smal, Wydawnictwo Wyższej Szkoły Oficerskiej Wojsk Lądowych, Wrocław 2015, s. 125.

technologie oraz specjalistyczny sprzęt są niezbędne do przeprowadzania działań ratunkowych w trudnych warunkach, w tym w obszarach zalanych, o utrudnionym dostępie. Stale rosnący postęp technologiczny, umożliwia łatwiejsze i szybsze podejmowanie decyzji podczas prowadzonych działań ratowniczo-gaśniczych[10].

Pompy są jednym z najważniejszych elementów wyposażenia wykorzystywanego przez PSP w walce z powodziami. Strażacy używają różnych typów pomp, które różnią się wydajnością i przeznaczeniem. W czasie powodzi, szczególnie w przypadku zalania budynków lub piwnic, kluczowe staje się jak najszybsze usunięcie wody, aby zapobiec dalszym uszkodzeniom infrastruktury oraz minimalizować zagrożenie dla mieszkańców. Pompy pożarnicze, w tym pompy wysokowydajne, pozwalają na usunięcie dużych ilości wody w krótkim czasie, co jest niezbędne w obliczu powodzi. W PSP wykorzystywane są różne rodzaje pomp: od małych, przenośnych pomp, które są w stanie przepompować wodę z zalanych piwnic, po ciężkie pompy, które mogą wydobywać wodę z zalanych ulic, obszarów przemysłowych czy terenów o dużej powierzchni. Pompy wysokiej wydajności, takie jak pompy typu „wersja pływająca", mogą być stosowane w trudnych warunkach terenowych, np. w miejscach, gdzie woda osiągnęła znaczny poziom. W Polsce funkcjonują dwa specjalistyczne moduły, w skład których wchodzą strażacy jednostek ratowniczo-gaśniczych. Jednym z modułów jest HCP. Moduł zawierający jednostki ratowniczo-gaśnicze, które mają na wyposażeniu pompy pożarnicze o wysokiej wydajności. Ich głównym założeniem funkcjonowania jest przepompowywanie i/lub przetłaczanie wody w dużych ilościach, na duże odległości[11]. Doskonale sprawdzają się podczas likwidacji skutków powodzi. Urządzenia te charakteryzują się zdolnością do pracy w ekstremalnych warunkach i w sytuacjach, gdzie woda występuje w dużych ilościach.

W obliczu powodzi, PSP regularnie wykorzystuje łodzie ratunkowe oraz pontony do przeprowadzania akcji ratunkowych. Łodzie te są niezastąpione w obszarach, gdzie ulice i inne drogi są całkowicie zalane, a dostęp do poszkodowanych osób jest możliwy jedynie przez wodę. Strażacy w takich sytuacjach używają specjalistycznych łodzi ratunkowych, które pozwalają na

[10] W. Gawroński, K. Tyrańska-Wizner, *Wykorzystanie geoinformacji przez Państwową Straż Pożarną*, Rocznik geomatyki, 2(64), 2014, s. 217.

[11] R. Podlasiński, Z. Ciekanowski, A. Radkevych, *Grupy ratownictwa specjalistycznego w Państwowej Straży Pożarnej*, De Securitate et Defensione. O Bezpieczeństwie i Obronności, nr 2, 2022, s. 157.

bezpieczne przemieszczanie się po wodzie oraz ratowanie osób znajdujących się w strefach zagrożenia. Ważnym elementem w czasie powodzi są również pontony, które ułatwiają przemieszczanie się po terenach zalanych, w tym w przypadku konieczności transportu osób lub sprzętu. Dzięki lekkiej konstrukcji i łatwości w transporcie, pontony mogą być wykorzystywane w terenach trudno dostępnych, w których inne pojazdy ratunkowe nie mają szans na dotarcie. Dodatkowo, są one niezbędne do transportu sprzętu ratunkowego, medycznego oraz do przeprowadzania ewakuacji ludzi w rejonach, gdzie inne środki transportu nie mogą być użyte. W działaniach związanych z powodziami, Państwowa Straż Pożarna korzysta także z nowoczesnego sprzętu do monitorowania i oceny sytuacji kryzysowej. Współczesne technologie pozwalają na zbieranie i analizowanie danych w czasie rzeczywistym, co umożliwia szybsze podejmowanie decyzji i skuteczniejsze zarządzanie akcją ratunkową. PSP wyposażona jest w systemy monitorowania poziomu wód, które umożliwiają ocenę zagrożenia na obszarach zalanych i prognozowanie dalszego rozwoju sytuacji. Państwowa Straż Pożarna czynnie włącza się w proces tworzenia nowych rozwiązań mających wspierać procesy decyzyjne, niezbędne podczas podejmowanych działań ratowniczo-gaśniczych[12].

Wykorzystanie dronów w monitorowaniu sytuacji powodziowej jest jednym z nowoczesnych rozwiązań, które stają się coraz bardziej popularne w służbach ratunkowych[13]. Dzięki dronom, strażacy mogą uzyskać obraz z powietrza, co pozwala na szybsze ocenienie skali zalania oraz identyfikację obszarów, które wymagają pilnej interwencji. Drony wyposażone w kamery termowizyjne mogą pomóc w wykrywaniu osób znajdujących się w trudno dostępnych miejscach, takich jak dachy budynków, jak również monitorowanie sytuacji w czasie szeroko pojętych wypadków komunikacyjnych, obserwację pożaru i ich analizę, co znacznie zwiększa efektywność działań ratunkowych. Ponadto, PSP korzysta z zaawansowanych systemów komunikacji i zarządzania kryzysowego, które umożliwiają wymianę informacji pomiędzy poszczególnymi jednostkami oraz koordynowanie działań w terenie. Dzięki tym systemom możliwe jest dokładne śledzenie sytuacji na poziomie lokalnym, a także

[12] M. Nepelski, *Wybrane technologie wspierające procesy decyzyjne w Państwowej Straży Pożarnej jako produkt prac badawczo-rozwojowych realizowanych na rzecz bezpieczeństwa powszechnego*, Zeszyty Naukowe SGSP, nr 79, 2021, s. 182.

[13] A. Michalski, *Nowoczesne technologie w bezpieczeństwie publicznym na przykładzie Państwowej Straży Pożarnej*, Security, Economy & Law, XXI, 2018, s. 34.

przesyłanie informacji o poziomie zagrożenia do centralnych jednostek koordynujących całą akcję ratunkową.

W przypadku powodzi, nie tylko same zalania, ale także zatory wodne stanowią poważne zagrożenie. Woda w rzekach, jeziorach czy innych zbiornikach może gromadzić się w wyniku blokady naturalnej lub sztucznej, co prowadzi do dalszego zagrożenia powodziowego. Aby temu zapobiec, PSP stosuje technologie wykorzystywane do usuwania takich przeszkód. Przykładem może być zastosowanie specjalistycznych wciągarek, urządzeń do cięcia drzew czy specjalnych narzędzi mechanicznych, które umożliwiają usuwanie przeszkód w korytach rzecznych lub na innych ciekach wodnych. W niektórych przypadkach PSP korzysta z technologii stosowanych do odblokowywania kanałów i dróg wodnych, co jest istotne, aby zapobiec dalszemu rozlewowi wody na terenach miejskich i wiejskich. Tego rodzaju technologia jest niezwykle skuteczna w walce z powodziami, ponieważ pozwala na szybsze udrożnienie szlaków wodnych, a tym samym minimalizowanie dalszych skutków wylewów.

Państwowa Straż Pożarna dysponuje także nowoczesnymi pojazdami ratunkowymi, które zostały dostosowane do warunków powodziowych. Pojazdy te, w tym samochody terenowe, specjalistyczne wozy ratunkowe i pojazdy opancerzone, są w stanie dotrzeć do miejsc, które zostały zalane lub zniszczone przez powódź. Wyposażenie tych pojazdów obejmuje nie tylko standardowy sprzęt ratunkowy, ale także narzędzia do pracy w trudnych warunkach terenowych, w tym w strefach podmokłych. Dzięki tym pojazdom, strażacy mogą szybko dotrzeć do poszkodowanych osób, nawet w najbardziej niedostępnych rejonach, zapewniając skuteczną pomoc[14]. Pojazdy te są również wyposażone w sprzęt do monitorowania stanu wód i oceniania skali zagrożenia, co pozwala na szybsze podejmowanie decyzji o ewentualnych akcjach ewakuacyjnych czy ratunkowych, ale również problem zbudowania takiego pojazdu wsparcia akcji ratowniczych prowadzonych w szczególnie trudnych warunkach, do których możemy zaliczyć:

- wyrzuty substancji toksycznych, produktów rozkładu termicznego lub spalania,
- bardzo silne promieniowanie cieplne i radiacyjne,

[14] J. Roguski, *Zastosowanie bezzałogowych statków powietrznych w straży pożarnej*, [w:] *Systemy bezzałogowych statków powietrznych w ochronie przeciwpożarowej i ratownictwie, - od wyrobu do ratownika. Rozważania teoretyczne a zastosowanie w rzeczywistości*, red. M. Feltynowski, Wydawnictwo CNBOP-PIB, Józefów 2022, s. 12.

- wysoka zmienność sytuacji i wystąpienie niespodziewanych zagrożeń, przy których wyposażenie ratowników w standardowe środki ochrony indywidualnej jest niewystarczające (o czym świadczą wypadki – również śmiertelne – wśród ratowników),
- konieczność prowadzenia działań na obszarach niedostępnych dla standardowych pojazdów ratowniczych[15].

Walka z zagrożeniami naturalnymi, w tym również powodziami, to zadanie wymagające zastosowania zaawansowanego sprzętu i technologii, które pozwalają na szybkie i skuteczne przeprowadzanie akcji ratunkowych. Państwowa Straż Pożarna wykorzystuje szeroki wachlarz urządzeń, takich jak pompy do usuwania wody, łodzie ratunkowe, drony, a także nowoczesne pojazdy ratunkowe. Dzięki tym technologiom, PSP jest w stanie skutecznie reagować na zagrożenia powodziowe, minimalizować straty i ratować życie ludzkie. W obliczu coraz częstszych zjawisk powodziowych, ciągłe inwestowanie w nowoczesny sprzęt oraz technologie monitorujące sytuację kryzysową, stanowi kluczowy element w utrzymaniu bezpieczeństwa obywateli.

Przykłady działań Państwowej Straży Pożarnej podczas powodzi

W dniach od 15 do 18 września 2024 roku województwo śląskie zostało dotknięte intensywnymi opadami deszczu, które spowodowały liczne powodzie i podtopienia. W odpowiedzi na te zagrożenia, Państwowa Straż Pożarna (PSP) podjęła szereg działań ratunkowych, angażując się w ewakuację mieszkańców, wypompowywanie wody z zalanych obszarów oraz monitorowanie stanu wałów przeciwpowodziowych. Przykładowe działania to m.in.

- w powiecie raciborskim strażacy skupili się na monitorowaniu wałów przeciwpowodziowych oraz zabezpieczaniu miejsc przecieków przy pomocy geowłókniny i worków z piaskiem. W miejscowościach Chałupki i Zabełków umocniono i wyrównano wały na rzece Odra, a w Kuźni Raciborskiej i Nędzy układano worki z piaskiem wzdłuż rzeki Ruda i Sumina;
- w powiecie pszczyńskim, w Goczałkowicach-Zdroju, strażacy przepompowywali wodę z zalanych terenów do koryta rzeki oraz umacniali kanał burzowy odprowadzający wodę do Jeziora Goczałkowickiego;

[15] Ibidem.

- w powiecie wodzisławskim strażacy doszczelniali wały zbiornika retencyjnego Polder Buków, aby zapobiec dalszym zalaniom[16].

W działaniach ratunkowych uczestniczyły również inne służby, takie jak policja, wojsko oraz organizacje pozarządowe. Współpraca ta była kluczowa dla skutecznej ewakuacji mieszkańców oraz zapewnienia pomocy osobom poszkodowanym. Strażacy nie tylko angażowali się w działania ratunkowe, ale także dostarczali artykuły pierwszej potrzeby osobom dotkniętym powodzią[17]. Poniżej przedstawiono powodziową statystykę sił biorących udział w działaniach:

- od 11 września br., Jednostki Ochronny Przeciwpożarowej (JOP) podjęły ponad 29 tys. interwencji związanych z powodzią, ewakuując przy tym ok. 4,5 tys. osób z terenów bezpośredniego zagrożenia;
- z jednostek ochrony przeciwpożarowej KSRG województw objętych działaniami powodziowymi, zaangażowanych zostało prawie 24 tys. pojazdów i 98 tys. ratowników;
- w ramach sił i środków Centralnego Odwodu Operacyjnego (COO) KG PSP zaangażowano 385 pojazdów i 1315 ratowników. Mając na uwadze, że codziennie w PSP służy ok. 5 tys. funkcjonariuszy – 1315 ratowników w ramach COO, to ponad 25% codziennego stanu osobowego PSP;
- dodatkowo, działając w oparciu o „Zasady postępowania służb dyżurnych stanowisk kierowania KW PSP oraz KP(M) PSP w przypadku otrzymania ostrzeżeń meteorologicznych lub hydrologicznych wydanych przez IMGW-PIB", zwiększono obsady w stanowiskach kierowania PSP oraz jednostkach ratowniczo- gaśniczych na terenie kraju o 6 866 funkcjonariuszy[18].

Strażacy stawiali czoła licznym trudnościom podczas akcji ratunkowych. Intensywne opady deszczu prowadziły do szybkiego wzrostu poziomu

[16] Działania związane z usuwaniem skutków powodzi w woj. śląskim - Komenda Wojewódzka Państwowej Straży Pożarnej w Katowicach - Portal Gov.pl, https://www.gov.pl/web/kwpsp-katowice/dzialania-zwiazane-z-usuwaniem-skutkow-powodzi-w-woj-slaskim, [dostęp: 29.01.2024 r.].

[17] *Powódź 2024. Straż pożarna dziękuje za współpracę: W obliczu tragicznych powodzi widzimy niesamowitą determinację,* TVN24, https://tvn24.pl/polska/powodz-2024-straz-pozarna-dziekuje-za-wspolprace-w-obliczu-tragicznych-powodzi-widzimy-niesamowita-determinacje-st8094516, [dostęp: 29.01.2024 r.].

[18] *Powodziowa statystyka interwencji oraz zaangażowanych sił i środków jednostek ochrony ppoż.*, Komenda Główna Państwowej Straży Pożarnej - Portal Gov.pl, https://www.gov.pl/web/kgpsp/powodziowa-statystyka-interwencji-oraz-zaangazowanych-sil-i-srodkow-jednostek-ochrony-ppoz, [dostęp: 29.01.2024 r.].

wód, co utrudniało dotarcie do poszkodowanych obszarów. Dodatkowo, zalane drogi i mosty ograniczały mobilność służb ratunkowych. Mimo tych wyzwań, strażacy wykazali się determinacją i profesjonalizmem, skutecznie ratując życie i mienie mieszkańców.

Doświadczenia z powodzi na Śląsku w 2024 roku pozwoliły na wyciągnięcie cennych wniosków dotyczących organizacji działań ratunkowych. Zidentyfikowano obszary wymagające usprawnień, takie jak lepsza koordynacja między służbami, szybsze reagowanie na zmieniające się warunki pogodowe oraz efektywniejsze wykorzystanie nowoczesnego sprzętu i technologii. Wnioski te stanowią podstawę do doskonalenia procedur i przygotowań na przyszłe zagrożenia powodziowe. Działania Państwowej Straży Pożarnej podczas powodzi na Śląsku w 2024 roku stanowią przykład skutecznej reakcji na kryzysowe sytuacje. Zaangażowanie strażaków, ich współpraca z innymi służbami oraz determinacja w ratowaniu mieszkańców, podkreślają znaczenie PSP w systemie zarządzania kryzysowego.

Podsumowanie

Państwowa Straż Pożarna odgrywa kluczową rolę w systemie zarządzania kryzysowego, zwłaszcza podczas powodzi, które są jednym z najpoważniejszych zagrożeń naturalnych w Polsce. Działania PSP obejmują zarówno interwencje ratunkowe, ewakuację mieszkańców, jak i zabezpieczanie infrastruktury, a także późniejsze usuwanie skutków kataklizmu. Nowoczesny sprzęt, technologie oraz ścisła współpraca z innymi służbami i instytucjami pozwalają na skuteczne minimalizowanie strat oraz ochronę życia i mienia obywateli.

Analizując sprzęt i technologie wykorzystywane przez PSP, można zauważyć, że strażacy są wyposażeni w nowoczesne narzędzia umożliwiające efektywną walkę z powodziami. Pompy wysokiej wydajności, łodzie ratunkowe, drony monitorujące oraz specjalistyczne pojazdy pozwalają na szybką reakcję i koordynację działań. Dzięki temu możliwe jest zarówno ratowanie osób znajdujących się w strefach zagrożenia, jak i skuteczne wypompowywanie wody oraz zabezpieczanie wałów przeciwpowodziowych.

Przykłady działań PSP podczas powodzi na Śląsku w 2024 roku pokazują, jak strażacy musieli zmierzyć się z wieloma wyzwaniami, takimi jak szybko rosnący poziom wód, ograniczona mobilność służb spowodowana zalaniem dróg oraz konieczność błyskawicznej ewakuacji mieszkańców. Współpraca

PSP z innymi podmiotami, w tym policją, wojskiem i organizacjami pozarządowymi, miała kluczowe znaczenie dla skuteczności działań ratunkowych. Mimo trudnych warunków strażacy wykazali się profesjonalizmem i determinacją, ratując życie ludzi oraz minimalizując straty materialne. Doświadczenia zdobyte podczas powodzi na Śląsku oraz innych podobnych katastrof naturalnych wskazują na kilka istotnych aspektów, które mogą przyczynić się do poprawy skuteczności działań PSP w przyszłości.

Przede wszystkim kluczowe jest dalsze inwestowanie w nowoczesny sprzęt ratunkowy oraz rozwijanie technologii umożliwiających lepsze monitorowanie sytuacji powodziowej. Drony, systemy wczesnego ostrzegania oraz zautomatyzowane mechanizmy oceny zagrożenia, pozwalają na szybsze reagowanie i bardziej precyzyjne podejmowanie decyzji. Drugim istotnym elementem jest doskonalenie procedur współpracy między różnymi służbami i instytucjami odpowiedzialnymi za zarządzanie kryzysowe. Skuteczna wymiana informacji, jasne zasady koordynacji działań oraz odpowiednie szkolenia dla strażaków i innych służb pozwolą na bardziej efektywne działanie w przyszłości.

W obliczu coraz częstszych i bardziej gwałtownych zjawisk pogodowych wynikających ze zmian klimatycznych, rola PSP w przeciwdziałaniu skutkom powodzi staje się jeszcze bardziej istotna. Konieczne jest dalsze rozwijanie infrastruktury przeciwpowodziowej, zwiększanie środków na nowoczesny sprzęt ratowniczy oraz edukacja społeczeństwa w zakresie postępowania w sytuacjach zagrożenia. W przyszłości istotne będzie również wykorzystanie nowych technologii, takich jak sztuczna inteligencja do analizowania zagrożeń powodziowych, automatyczne systemy powiadamiania ludności oraz jeszcze bardziej zaawansowane drony i roboty do działań w ekstremalnych warunkach.

Podsumowując, działania Państwowej Straży Pożarnej podczas powodzi stanowią nieoceniony element systemu bezpieczeństwa i zarządzania kryzysowego. Dzięki odpowiedniemu wyposażeniu, współpracy z innymi służbami oraz zaangażowaniu strażaków, możliwe jest skuteczne ograniczanie skutków kataklizmów. Jednak, aby zapewnić jeszcze większą efektywność w przyszłości, konieczne są dalsze inwestycje, szkolenia oraz rozwój technologii, które pozwolą na jeszcze szybsze i bardziej precyzyjne działania ratunkowe.

Literatura

1. Ciekanowski Z., Żurawski S., *Państwowa Straż Pożarna jako grupa dyspozycyjna w systemie zarządzania kryzysowego*, Aviation and Security Issues, nr 1(1), 2022.
2. *Działania związane z usuwaniem skutków powodzi w woj. śląskim*, Komenda Wojewódzka Państwowej Straży Pożarnej w Katowicach, Portal Gov.pl, https://www.gov.pl/web/kwpsp-katowice/dzialania-zwiazane-z-usuwaniem-skutkow-powodzi-w-woj-slaskim.
3. Filaber J., *Działania ratownicze ochotniczych straży pożarnych podczas akcji ratowniczych organizowanych i prowadzonych przez Państwową Straż Pożarną*, „Acta Universitatis Wratislaviensis", no. 3861, 2018.
4. Gawroński W., Tyrańska-Wizner K., *Wykorzystanie geoinformacji przez Państwową Straż Pożarną*, Rocznik geomatyki, 2(64), 2014.
5. Gromek P., *Państwowa Straż Pożarna a zarządzanie kryzysowe. Ujęcie strukturalne*, Zeszyty Naukowe SGSP, nr 63/3, 2017.
6. Księga dobrych praktyk w zakresie zarządzania ciągłością działania, red. R.W. Kaszubski, D. Romańczuk, Wydawnictwo FTB przy ZBP, Warszawa 2012.
7. Michalski A., *Nowoczesne technologie w bezpieczeństwie publicznym na przykładzie Państwowej Straży Pożarnej*, Security, Economy & Law, XXI, 2018.
8. Misterka M., *Analiza działań Państwowej Straży Pożarnej podczas powodzi w 2010 roku w świetle usprawniania ochrony przeciwpowodziowej w Polsce – część 1*, Zeszyty Naukowe SGSP, nr 56(4) 2015.
9. Nepelski M., *Wybrane technologie wspierające procesy decyzyjne w Państwowej Straży Pożarnej jako produkt prac badawczo-rozwojowych realizowanych na rzecz bezpieczeństwa powszechnego*, Zeszyty Naukowe SGSP, nr 79, 2021.
10. Pietrek G., *Krajowy System Ratowniczo-Gaśniczy-zasadniczy element podsystemu wykonawczego zarządzania kryzysowego. Wnioski z powodzi 2010 rok*, [w:] *Systemy ratownicze w Polsce a bezpieczeństwo cywilne i wojskowe*, red. B. Zysiak-Christ, T. Smal, Wydawnictwo Wyższej Szkoły Oficerskiej Wojsk Lądowych, Wrocław 2015.
11. Podlasiński R., Ciekanowski Z., Radkevych A., *Grupy ratownictwa specjalistycznego w Państwowej Straży Pożarnej*, De Securitate et Defensione. O Bezpieczeństwie i Obronności, nr 2, 2022.
12. *Podsumowanie działań prewencji społecznej*, Komenda Główna Państwowej Straży Pożarnej.
13. Powódź 2024. Straż pożarna dziękuje za współpracę: W obliczu tragicznych powodzi widzimy niesamowitą determinację - TVN24, https://tvn24.pl/polska/powodz-2024-straz-pozarna-dziekuje-za-wspolprace-w-obliczu-tragicznych-powodzi-widzimy-niesamowita-determinacje-st8094516/.
14. *Powodziowa statystyka interwencji oraz zaangażowanych sił i środków jednostek ochrony ppoż*., Komenda Główna Państwowej Straży Pożarnej - Portal Gov.pl, https://www.gov.pl/web/kgpsp/powodziowa-statystyka-interwencji-oraz-zaangazowanych-sil-i-srodkow-jednostek-ochrony-ppoz.

15. Roguski J., *Zastosowanie bezzałogowych statków powietrznych w straży pożarnej*, [w:] *Systemy bezzałogowych statków powietrznych w ochronie przeciwpożarowej i ratownictwie, - od wyrobu do ratownika. Rozważania teoretyczne a zastosowanie w rzeczywistości*, red. M. Feltynowski, Wydawnictwo CNBOP-PIB Józefów 2022.
16. Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. 1991 Nr 88, poz. 400).
17. Zalewska K., Ochyra-Żurawska K., Ciekanowski Z., *Organizacje pozarządowe w systemie bezpieczeństwa państwa*, Studia Administracji i Bezpieczeństwa, 13(13), 2022.

dr inż. Tomasz Grudniewski
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0003-3394-8992
https://doi.org/10.29316/9788368103199_12

INTEGRACJA FOTOWOLTAIKI WSPIERANEJ SZTUCZNĄ INTELIGENCJĄ W STRATEGIACH BEZPIECZEŃSTWA ENERGETYCZNEGO PAŃSTW

AI-SUPORTED PHOTOVOLTAICS IN NATIONAL ENERGY SECURITY STRATEGIES

Streszczenie

Celem rozdziału jest zbadanie, w jaki sposób różne państwa uwzględniają fotowoltaikę wspomaganą sztuczną inteligencją (AI) w swoich strategiach bezpieczeństwa energetycznego. Centralny problem badawczy dotyczy efektywnego włączenia technologii AI do rozwoju i zarządzania systemami fotowoltaicznymi, tak aby zwiększyć niezawodność dostaw, obniżyć koszty i jednocześnie ograniczyć ryzyka, w tym zagrożenia cybernetyczne. W tym kontekście przeanalizowano dokumenty strategiczne i regulacyjne (m.in. USA, UE, Chiny), konfrontując je z literaturą przedmiotu oraz raportami międzynarodowych organizacji (IEA, REN21). Metodologicznie zastosowano wieloaspektowe podejście: analizę jakościową dokumentów, studium przypadku wybranych państw oraz porównawczą syntezę wniosków. Dzięki

Summary

The chapter aims to investigate how various countries incorporate photovoltaics supported by artificial intelligence (AI) into their energy security strategies. The central research question focuses on the effective integration of AI technology into photovoltaic development and management to enhance supply reliability, reduce costs, and simultaneously address associated risks, including cyber threats. In this context, the study examines strategic and regulatory documents (e.g., from the U.S., EU, China) in light of existing literature and reports from international organizations (IEA, REN21). Methodologically, a multi-faceted approach was employed: qualitative document analysis, case studies of selected nations, and a comparative synthesis of findings. This approach provided a comprehensive view of current practices and challenges related

temu uzyskano pełniejszy obraz aktualnych praktyk i wyzwań związanych z integracją fotowoltaiki i AI. Wyniki analiz wskazują, że choć poszczególne kraje rozpoznają rosnące znaczenie tej technologii, to poziom formalnego uwzględnienia AI w politykach bezpieczeństwa energetycznego jest zróżnicowany. Na tej podstawie przedstawiono rekomendacje strategiczne, dotyczące m.in. ram regulacyjnych, inwestycji w infrastrukturę cyfrową i kształcenia kadr, a także postulat szerszej współpracy międzynarodowej w zakresie cyberbezpieczeństwa i standardów dla inteligentnych sieci.

Słowa kluczowe: fotowoltaika, sztuczna inteligencja, bezpieczeństwo energetyczne, inteligentne sieci, polityka energetyczna

to the integration of photovoltaics and AI. The results indicate that, although individual countries recognize the growing importance of such technologies, the formal inclusion of AI in energy security policies varies widely. Based on these observations, strategic recommendations are offered, addressing regulatory frameworks, investments in digital infrastructure and workforce development, as well as the need for broader international cooperation on cybersecurity and intelligent-grid standards.

Keywords: photovoltaics, artificial Intelligence, energy security, smart grids, energy policy

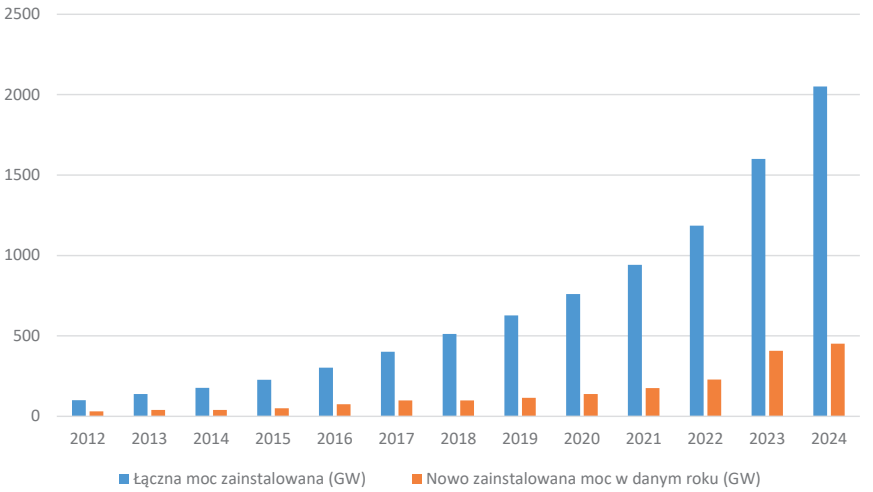
Wstęp

Transformacja energetyczna i rozwój odnawialnych źródeł energii (OZE) stały się kluczowym wymiarem polityki gospodarczej i bezpieczeństwa narodowego w XXI wieku. Bezpieczeństwo energetyczne tradycyjnie oznacza zdolność państwa do zapewnienia nieprzerwanego dostępu do energii po akceptowalnej cenie oraz ochrony przed zakłóceniami dostaw. Przez dekady koncentrowało się ono na zabezpieczeniu dostaw paliw kopalnych (ropy, gazu, węgla) i stabilności sieci elektroenergetycznej. Współcześnie nabiera jednak nowego znaczenia w obliczu dążenia do gospodarki niskoemisyjnej i rozproszonej produkcji energii. Fotowoltaika (PV) – najszybciej rosnące źródło energii elektrycznej ostatnich lat – odgrywa główną rolę w tym procesie. Globalna moc zainstalowana instalacji fotowoltaicznych przekroczyła już 1,6 terawata (TW) na koniec 2023 roku (wzrost z ok. 1,2 TW rok wcześniej), co oznacza, że energia słoneczna odpowiada za ponad 6% światowej produkcji elektryczności[1,2]. Dla porównania, w 2012 r. moc PV wynosiła zaledwie 0,1 TW. Taki skok ilustruje rysunek 1. Państwa dostrzegają szansę na dywersyfikację źródeł i częściowe uniezależnienie się od importowanych surowców, dzięki energii

[1] IEA-PVPS (2024) – IEA Photovoltaic Power Systems Programme, *Snapshot of Global PV Markets 2023*, Report IEA-PVPS T1-42:2024, 2024.

[2] REN21 – *Renewables 2023 Global Status Report* – REN21 (Paris: REN21 Secretariat). 2023.

słonecznej. Co więcej, energia z dużych farm fotowoltaicznych stała się jedną z najtańszych form pozyskiwania elektryczności, przyciągając rekordowe inwestycje rzędu 0,5 bln USD w 2022 roku w skali świata[3].



Rysunek 1. Globalna zainstalowana i prognozowana (2024) moc fotowoltaiczna i roczne przyrosty w latach 2012–2024 (opracowanie własne na podstawie danych IEA-PVPS[3] i REN21[4])

Źródło: opracowanie własne.

Jednocześnie dynamiczny rozwój źródeł odnawialnych wiąże się z nowymi wyzwaniami technologicznymi i strategicznymi. W systemie energetycznym opartym w większym stopniu na energii słonecznej i wiatrowej rośnie znaczenie rozwiązań zapewniających elastyczność sieci, zdolność bilansowania podaży i popytu w czasie rzeczywistym oraz odporność na zakłócenia. W integracji rozproszonych, zależnych od pogody źródeł OZE coraz większą rolę odgrywa cyfryzacja i sztuczna inteligencja (SI, AI). Dzięki analizie ogromnych zbiorów danych i uczeniu maszynowemu, algorytmy AI mogą optymalizować zużycie energii, poprawiać stabilność sieci i wspomagać podejmowanie decyzji w czasie rzeczywistym[5]. Sztuczna inteligencja jest postrzegana jako technologia o przełomowym potencjale dla sektora energii – może przyspieszyć innowacje,

[3] IEA-PVPS (2024) – IEA *Photovoltaic Power Systems Programme, Snapshot of Global PV Markets* 2023, Report IEA-PVPS T1-42:2024, 2024.

[4] REN21 – *Renewables 2023 Global Status Report – REN21* (Paris: REN21 Secretariat). 2023.

[5] WEF – Al-Zu'bi, I., "*Energy and AI: the power couple that could usher in a net-zero world*", World Economic Forum, 2025.

zwiększyć efektywność systemów elektroenergetycznych oraz wzmocnić bezpieczeństwo energetyczne dostaw[6]. Co więcej, stała się technologią transformacyjną usprawniającą każdy element systemu energetycznego – od integracji OZE po stabilizację sieci[7]. Według analiz Międzynarodowej Agencji Energetycznej (IEA) zastosowanie AI i zaawansowanej analityki danych w energetyce może przynieść do 2030 roku nawet 1,3 bln USD wartości ekonomicznej dzięki poprawie efektywności i nowym modelom biznesowym, a globalna emisja CO_2 mogłaby spaść o 5-10% (co odpowiada rocznej emisji całej Unii Europejskiej)[8]. AI umożliwia m.in. precyzyjne prognozowanie generacji fotowoltaiki i popytu, automatyczne sterowanie popytem (np. urządzeniami domowymi czy ładowaniem pojazdów elektrycznych), a także predykcyjną konserwację infrastruktury – identyfikując awarie paneli czy falowników zanim spowodują one przerwy w dostawach. Zgodnie z najnowszymi badaniami, AI oferuje również „rewolucyjne rozwiązania" usprawniające integrację OZE, zarządzanie magazynami energii i bezpieczeństwo sieci[9].

Wszystko to sprawia, że fotowoltaika wspierana sztuczną inteligencją jawi się jako strategiczne połączenie mogące zarówno wspomóc osiągnięcie celów klimatycznych, jak i zwiększyć niezawodność oraz bezpieczeństwo dostaw energii w państwach na całym świecie. Nic więc dziwnego, że coraz więcej rządów i organizacji międzynarodowych pochyla się nad kwestią integracji cyfrowych innowacji w sektorze energetycznym. Komisja Europejska w 2022 r. przyjęła Plan działań UE na rzecz cyfryzacji systemu energetycznego, wskazując, że nowe technologie (w tym IoT i AI) są kluczowe, by efektywnie wykorzystywać zasoby energii i zwiększyć udział OZE w mixie energetycznym – co stało się pilne w obliczu kryzysu cenowego i konieczności uniezależnienia się od importu paliw kopalnych[10]. Podobnie w skali globalnej IEA zainicjowała w 2024 r. program „Energy for AI, AI for Energy", podkreślając potrzebę współpracy rządów, sektora energii i technologii w celu bezpiecznej

[6] IEA – Birol, F., Press Release: "*IEA's first major Global Conference on Energy & AI*", International Energy Agency, 2024.

[7] Y. Wang, X. Zhao, J. Martin, S. Liu, *The role of AI in accelerating the adoption of intermittent renewable energies*. Energy Strategy Reviews, 40, 103045. 2025.

[8] WEF (2025) – Al-Zu'bi, I., "*Energy and AI: the power couple that could usher in a net-zero world*", World Economic Forum, 2025.

[9] H. Chen, J. Park, Q. Li, *Revolutionizing solar PV integration: AI-driven forecasting and grid stability*. Energy, 263, 125879. 2025.

[10] European Commission – "*Digitalising the energy system – EU Action Plan*", Komunikat COM(2022) 552 final, Brussels, 2022.

i efektywnej cyfryzacji energetyki. Jak ujął to dyrektor wykonawczy IEA Fatih Birol: „Nie ma AI bez energii – szczególnie elektryczności. […] Jednocześnie AI może być technologią transformacyjną dla sektora energii, z potencjałem poprawy efektywności i bezpieczeństwa, przyspieszenia transformacji”[11]. Na tym tle wyłania się pytanie o to, czy i jak rządy państw uwzględniają fotowoltaikę wspieraną AI w swoich strategiach bezpieczeństwa energetycznego. Niniejszy rozdział podejmuje tę problematykę, analizując globalne podejścia strategiczne do integracji PV+AI, identyfikując najlepsze praktyki oraz luki polityczne, a także formułując rekomendacje.

Celem niniejszego rozdziału jest przeanalizowanie, w jaki sposób państwa na świecie uwzględniają fotowoltaikę wspomaganą sztuczną inteligencją w swoich strategiach bezpieczeństwa energetycznego. Analiza ma na celu zidentyfikowanie najlepszych praktyk politycznych i strategicznych w integrowaniu nowych technologii (PV + AI) w politykach energetycznych, a jednocześnie wskazanie luk i braków w obecnych strategiach. Na tej podstawie sformułowane zostaną rekomendacje dla decydentów – zarówno na poziomie krajowym, jak i międzynarodowym – odnośnie do działań niezbędnych dla efektywnego wykorzystania synergii fotowoltaiki i AI w umacnianiu bezpieczeństwa dostaw energii. Główny problem badawczy można sformułować następująco: W jaki sposób fotowoltaika wspierana sztuczną inteligencją może zostać efektywnie zintegrowana z narodowymi strategiami bezpieczeństwa energetycznego oraz jakie korzyści i wyzwania strategiczne wiążą się z taką integracją? Innymi słowy: czy rządy adekwatnie reagują na rozwój PV i AI w kontekście bezpieczeństwa dostaw energii, czy też istnieje potrzeba aktualizacji i wzmocnienia strategii energetycznych o te nowe elementy? Rozwiązanie tego problemu wymaga ustalenia, czy i gdzie polityki energetyczne uwzględniają (bądź pomijają) zastosowania AI na różnych etapach łańcucha wartości fotowoltaiki – od prognozowania produkcji, przez sterowanie siecią i magazynowanie, po obsługę odbiorców. Badanie dotyczy również bilansu korzyści (np. lepsze prognozy i stabilność dostaw, zwiększenie udziału energii słonecznej, obniżenie kosztów) oraz ryzyka (np. cyberbezpieczeństwo, zależność od dostawców technologii, koszty wdrożeń) związanych z integracją PV+AI w skali państwa. W celu realizacji powyższego problemu i odpowiedzi na postawiony cel badawczy zastosowano wieloaspektowe podejście

[11] IEA – Birol, F., Press Release: “*IEA’s first major Global Conference on Energy & AI*”, International Energy Agency, 2024.

badawcze. Po pierwsze, przeprowadzono analizę literatury przedmiotu, obejmującą najnowsze publikacje naukowe oraz raporty uznanych organizacji (m.in. IEA, IRENA, REN21) dotyczące cyfryzacji energetyki, zastosowań AI w OZE oraz polityk energetycznych. Szczególną uwagę poświęcono raportom strategicznym i prognostycznym, takim jak raport RAND Corporation z 2024 r. dotyczącym wykorzystania AI dla poprawy bezpieczeństwa energetycznego, a także opracowaniom Międzynarodowej Agencji Energetycznej (np. komentarze analityczne IEA na temat AI w energetyce)[12]. Po drugie, dokonano analizy dokumentów strategicznych i regulacyjnych wybranych państw i regionów: przeanalizowano krajowe polityki energetyczne (m.in. strategie bezpieczeństwa energetycznego USA, Chin, Wielkiej Brytanii), strategie rozwoju AI oraz dokumenty UE (np. Plan działań UE na rzecz cyfryzacji systemu energii 2022, projekt Rozporządzenia UE w sprawie AI)[13]. Wykorzystano również dane statystyczne (dot. mocy zainstalowanej PV, udziału OZE, itp.) z raportów REN21 i IEA-PVPS, co pozwoliło osadzić rozważania w kontekście aktualnej struktury rynku PV. Po trzecie, zastosowano studium przypadku w ujęciu porównawczym: prześledzono i zestawiono podejścia do integracji PV+AI m.in. w Stanach Zjednoczonych, Unii Europejskiej (oraz wybranych państwach członkowskich, jak Niemcy czy Polska), Chinach, a także w zarysie w innych krajach wyróżniających się w tych obszarach (np. Japonii, Australii). Takie podejście umożliwia dostrzeżenie różnic i podobieństw – np. między państwami wiodącymi technologicznie a rozwijającymi się. Analiza objęła także inicjatywy międzynarodowe dotyczące AI w energetyce, w tym działania IEA, OECD oraz partnerstw publiczno-prywatnych (np. WEF Energy Transition Index i inicjatywy typu Mission Innovation). Wyniki tych analiz zostały poddane syntezie w celu sformułowania wniosków i rekomendacji.

Fotowoltaika, sztuczna inteligencja i bezpieczeństwo energetyczne – związek i znaczenie

Integrowanie fotowoltaiki z rozwiązaniami sztucznej inteligencji niesie ze sobą potencjał podniesienia bezpieczeństwa energetycznego państw na kilka

[12] RAND (2024) – Nouwens, Meiser et al., "*The use of AI for improving energy security: Exploring risks and opportunities in the electricity system*", RAND Corporation Research Report RRA2907-1, 2024.

[13] European Commission – *Digitalising the energy system – EU Action Plan*, Komunikat COM(2022) 552 final, Brussels, 2022.

sposobów. Przede wszystkim PV+AI może zwiększyć niezawodność i odporność systemu energetycznego. Tradycyjnie stabilność sieci elektrycznej opierała się na sterowaniu produkcją w dużych, centralnych elektrowniach, podczas gdy OZE (jak fotowoltaika) wprowadzają do systemu zmienność i nieprzewidywalność produkcji zależnej od warunków pogodowych. Dzięki AI ta nieprzewidywalność może być skuteczniej opanowana: algorytmy uczące się na podstawie danych meteorologicznych i historycznych są w stanie z dużą dokładnością prognozować nasłonecznienie i generację PV nawet z kilkudziesięciogodzinnym wyprzedzeniem. Przykładowo, firma Google wraz z DeepMind opracowała sieć neuronową do przewidywania produkcji swoich farm wiatrowych z 36-godzinnym wyprzedzeniem – zwiększając wartość energii sprzedawanej na rynku o 20% dzięki lepszemu planowaniu dostaw. Podobne podejścia stosuje się do farm fotowoltaicznych – precyzyjny forecasting pozwala operatorom sieci wcześniej reagować (np. uruchamiać rezerwy) i zapobiegać niedoborom mocy. Z kolei na poziomie odbiorców końcowych, inteligentne liczniki i systemy zarządzania popytem potrafią automatycznie dostosować zużycie – np. włączać bojlery czy ładowanie baterii właśnie wtedy, gdy świeci słońce i energia PV jest najobficiej dostępna. Takie zarządzanie popytem z wykorzystaniem AI („demand response") zmniejsza szczytowe obciążenia i ryzyko przeciążeń, wzmacniając pewność dostaw. Integracja AI podnosi też niezawodność odnawialnych źródeł energii oraz efektywność ich wykorzystania, wspierając bezpieczeństwo energetyczne i cele zrównoważonego rozwoju[14].

AI przyczynia się również do dywersyfikacji źródeł i lepszego wykorzystania istniejących zasobów energii słonecznej. Dzięki technikom uczenia maszynowego możliwe jest bardziej efektywne sterowanie dużymi zbiorowościami rozproszonych instalacji PV – tworzenie tzw. wirtualnych elektrowni (VPP). Wirtualna elektrownia to platforma, która inteligentnie zarządza i agreguje generację, magazynowanie oraz zużycie energii w rozproszonej sieci prosumentów, reagując na sygnały rynkowe i potrzeby systemu. AI stanowi mózg takiego systemu, decydując, kiedy gromadzić energię (np. ładować domowe baterie lub akumulatory samochodów elektrycznych), a kiedy oddawać ją do sieci, aby zmaksymalizować zarówno korzyści dla właścicieli instalacji, jak i stabilność sieci[15]. Dobrze zaprojektowane VPP mogą pełnić funkcje podobne

[14] S. Raman, S. Kumari, A. Ortiz, *Synergizing AI and renewables to achieve SDG7: A global assessment of energy security and sustainability*. Sustainability, 16(8), 4501, 2024.

[15] WEF (2025) – Al-Zu'bi, I., "*Energy and AI: the power couple that could usher in a net-zero world*", World Economic Forum, 2025.

do tradycyjnych elektrowni – dostarczając moc w szczycie zapotrzebowania lub wspomagając regulację częstotliwości – ale złożone są z tysięcy małych, rozproszonych źródeł PV, magazynów i odbiorników. Australijskie i europejskie projekty VPP pokazują, że z pomocą AI możliwe jest uzyskanie wysokiej efektywności takich rozwiązań i zapewnienie, że duży udział PV w miksie nie zagrozi bezpieczeństwu dostaw energii (np. inicjatywy opisywane przez delfos.energy). Dzięki AI możliwa jest również dynamiczna integracja niestabilnych źródeł, redukcja obciążenia sieci w szczytach oraz unikanie przerw w zasilaniu[16].

Kolejnym aspektem jest obniżanie kosztów operacyjnych i poprawa efektywności dzięki AI. Utrzymanie farm fotowoltaicznych i sieci wymaganej do integracji dużej mocy PV generuje nowe wyzwania – np. konieczność monitoringu dziesiątek tysięcy paneli czy setek inwerterów w czasie rzeczywistym. Zastosowanie kamer termowizyjnych i dronów wyposażonych w algorytmy rozpoznawania obrazów (AI) pozwala automatycznie wykrywać uszkodzone lub zabrudzone moduły, zanim spowodują spadek wydajności. Predykcyjne utrzymanie ruchu (predictive maintenance) oparte na AI identyfikuje wzorce wskazujące przyszłe awarie transformatorów, połączeń czy baterii, co umożliwia zaplanowanie napraw i uniknięcie awaryjnych przestojów. W konsekwencji, farmy PV działają z wyższą dyspozycyjnością, a sieć elektroenergetyczna jest mniej narażona na nagłe zakłócenia – co bezpośrednio przekłada się na bezpieczeństwo dostaw. AI umożliwia przełomową poprawę efektywności i stabilności pracy instalacji PV, przewyższając tradycyjne metody[17]. Nie można zapominać, że AI wspiera także długoterminowe planowanie i politykę energetyczną. Dzięki zaawansowanym modelom optymalizacyjnym, decydenci mogą symulować różne scenariusze rozwoju fotowoltaiki (np. rozmieszczenia geograficzne instalacji, poziom autokonsumpcji prosumentów) i oceniać ich wpływ na bezpieczeństwo systemu. AI potrafi przetwarzać ogromne zbiory danych – od meteorologii, przez profile zużycia, po ceny rynkowe – wskazując najbardziej efektywne inwestycje zwiększające bezpieczeństwo energetyczne (np. lokalizacje magazynów energii buforujących wahania PV). Wreszcie, sztuczna inteligencja może pomóc w wykrywaniu zagrożeń dla

[16] R. Balamurugan, M. Huang, D. Kim, H. Amano, *Smart Grids and Artificial Intelligence: Enabling large-scale solar and wind penetration*. Frontiers in Energy Research, 13, 1155337. 2025.

[17] X. Tian, A. Foong, T. Nguyen, *Artificial Intelligence Applications in Photovoltaic Systems: A Comprehensive Review*. CAAI Artificial Intelligence Research, 11(2), 2024, s. 146-160.

bezpieczeństwa – np. anomalie w sygnałach sterujących mogą wskazywać na cyberatak na farmę fotowoltaiczną lub system zdalnego sterowania (SCADA) sieci[18]. W dobie rosnącego ryzyka cyberzagrożeń dla infrastruktury krytycznej, zdolność AI do natychmiastowego rozpoznania nietypowych wzorców i aktywacji procedur obronnych jest nieoceniona.

Podsumowując, fotowoltaika wspierana AI może wzmacniać filary bezpieczeństwa energetycznego: dostępność (bo większy potencjał OZE dostępny lokalnie), przystępność cenową (optymalizacja kosztów i efektywności), oraz odporność (inteligentne reagowanie na zakłócenia i ataki). AI przyczynia się do tworzenia odpornych, niskoemisyjnych systemów energetycznych o wysokiej efektywności kosztowej, co jest kluczowe dla bezpieczeństwa dostaw[19]. Jednak skala tych korzyści zależy od odpowiedniego wdrożenia technologii oraz ram politycznych sprzyjających cyfryzacji energetyki. W kolejnych częściach przyjrzymy się, jak poszczególne państwa i regiony podchodzą do integracji PV+AI w swoich strategiach.

Strategie wybranych państw w zakresie PV i AI – najlepsze praktyki i luki

Stany Zjednoczone są jednym z globalnych liderów zarówno pod względem zainstalowanej mocy fotowoltaicznej, jak i rozwoju sztucznej inteligencji. Pod koniec 2022 roku USA posiadały ok. 142 GW mocy PV (drugie miejsce na świecie po Chinach), co stanowiło nieco ponad 12% udziału w globalnej mocy PV[20]. Mimo imponującego rozwoju energetyki słonecznej, analiza dokumentów strategicznych USA pokazuje, że integracja AI w polityce energetycznej dopiero raczkuje. Kluczowe dokumenty dotyczące bezpieczeństwa energetycznego – takie jak federalna ustawa Energy Security and Independence Act z 2022 r. czy Strategia Energetyczna Departamentu Obrony USA z 2023 r. – nie wspominają explicite o sztucznej inteligencji. Oznacza to, że kwestie cyfryzacji i inteligentnego zarządzania siecią nie zostały wprost uwzględnione w narracji o bezpieczeństwie dostaw.

[18] RAND (2024) – Nouwens, Meiser et al., "*The use of AI for improving energy security: Exploring risks and opportunities in the electricity system",* RAND Corporation Research Report RRA2907-1, 2024.

[19] G. Kyriakarakos (ed.), *AI, clean energy, and the resilience of future power systems*. Sustainability, 17(3), 1987. 2025.

[20] REN21 – *Renewables 2023 Global Status Report – REN21* (Paris: REN21 Secretariat). 2023.

Nie znaczy to jednak, że w USA brakuje inicjatyw łączących AI i energetykę. Wręcz przeciwnie – działania te toczą się na poziomie agencji rządowych i programów badawczych. Departament Energii (DoE) USA prowadzi aktywne prace nad zastosowaniami AI w sektorze energii, m.in. poprzez specjalne jednostki organizacyjne. W 2019 r. utworzono w DoE Biuro ds. Sztucznej Inteligencji i Technologii (AITO), którego celem jest koordynacja badań i wdrożeń AI w projektach energetycznych. DoE opracował też ramy zarządzania ryzykiem AI (AI Risk Management Playbook) dla zastosowań w energetyce. Co istotne, Kongres USA uchwalił National AI Initiative Act (2020) ustanawiając programy wsparcia badań AI w różnych sektorach, w tym w energetyce – wskazując DoE jako jeden z filarów tych działań. Mimo że przepisy energetyczne nie wymieniają AI, to administracja podejmuje kroki, by włączyć AI do praktyki zarządzania siecią. Symbolicznym zwrotem ku integracji technologii był Rozkaz Wykonawczy Prezydenta USA z października 2023 r. dotyczący AI, który zobowiązał Sekretarza Energii USA do przygotowania publicznego raportu o tym, jak AI może usprawnić planowanie, inwestycje i operacje sieci elektroenergetycznej. To pierwszy tak bezpośredni sygnał na szczeblu najwyższym, że AI jest postrzegana jako element przyszłego systemu energetycznego kraju. W praktyce, w USA trwają liczne projekty pilotażowe z zakresu inteligentnych sieci (smart grids) i magazynowania energii sterowanego AI. Kilka stanów (m.in. Kalifornia, Hawaje, Nowy Jork) promuje inicjatywy wirtualnych elektrowni zarządzanych przez algorytmy – np. łączenie domowych magazynów Tesla Powerwall w sieci reagujące na zapotrzebowanie. Operatorzy systemów energetycznych (ISO/RTO) coraz częściej korzystają z narzędzi analitycznych AI do prognoz obciążenia i wykrywania anomalii w pracy sieci. Najlepszą praktyką w USA jest z pewnością intensywny rozwój partnerstw publiczno-prywatnych – np. współpraca DoE z firmami z Doliny Krzemowej nad aplikacjami AI do optymalizacji pracy inwerterów PV czy dynamicznego sterowania falownikami w warunkach przeciążeń. Amerykańska strategia charakteryzuje się więc oddolnym, technologicznym podejściem – „de facto" integracją PV+AI, choć brakuje jeszcze spójnej narracji politycznej łączącej te obszary. Luką pozostaje brak zaktualizowanej strategii bezpieczeństwa energetycznego, która uwzględniałaby rozwój OZE i cyfryzację jako elementy zwiększające odporność systemu. Wydaje się, że jest to kierunek, w którym w najbliższych latach USA będą musiały pójść, zwłaszcza w obliczu realizacji ambitnych celów klimatycznych (100% czystej energii elektrycznej do 2035 r.) i związanej z tym konieczności istotnej przebudowy sieci.

Unia Europejska

Unia Europejska jako blok gospodarczy, dysponuje łącznie zbliżoną mocą fotowoltaiki co Stany Zjednoczone – na koniec 2022 r. kraje UE miały łącznie ponad 208 GW mocy PV (najwięcej: Niemcy ok. 67 GW, Hiszpania 26 GW, Włochy 25 GW, Francja 18 GW, Niderlandy 18 GW)[21]. UE wyróżnia się jednak systemowym podejściem do transformacji energetycznej i cyfryzacji. Integracja inteligentnych technologii w energetyce jest explicite częścią polityk UE, choć dokonuje się to kilkoma równoległymi ścieżkami. Przede wszystkim Unia finalizuje obecnie pierwsze w świecie kompleksowe prawo dotyczące AI – Akt o Sztucznej Inteligencji (AI Act). Projekt tego rozporządzenia (procedowany od 2021 r.) przyjmuje podejście oparte na ocenie ryzyka i wprost wymienia zastosowania AI w zarządzaniu sieciami elektroenergetycznymi jako obszary wysokiego ryzyka, podlegające ostrzejszym wymogom bezpieczeństwa i certyfikacji. Oznacza to, że UE już na etapie regulowania AI przewiduje jej kluczową rolę w infrastrukturze energetycznej – wiążąc ją z kwestią bezpieczeństwa (rozumianego także jako bezpieczeństwo użytkowników i stabilność dostaw).

Z drugiej strony, polityka energetyczna UE akcentuje cyfryzację jako środek do osiągnięcia celów bezpieczeństwa i zrównoważenia. W ramach Europejskiego Zielonego Ładu wskazano cyfryzację jako jeden z filarów transformacji (obok OZE i efektywności). W 2022 r. Komisja Europejska ogłosiła wspomniany Action Plan on Digitalising the Energy System, który zawiera szereg działań – od wspólnych przestrzeni danych energetycznych, przez wsparcie rozwoju sieci inteligentnych, po wzmocnienie cyberbezpieczeństwa sektora energii[22]. Plan ten powstał w reakcji na kryzys wywołany rosyjską agresją na Ukrainę – cyfryzacja ma pomóc "zakończyć zależność UE od rosyjskich paliw kopalnych i sprostać kryzysowi klimatycznemu", m.in. poprzez większe wykorzystanie lokalnych OZE. Jest to wyraźny przykład uznania, że fotowoltaika wraz z inteligentnym zarządzaniem (AI), to nie tylko kwestia innowacji, ale i geostrategicznej odporności. W planie podkreślono, że do integracji masowego napływu OZE niezbędne są nowinki cyfrowe – inteligentne budynki, liczniki, urządzenia IoT zbierające dane o zużyciu i generacji, a także nowe usługi i aplikacje dla prosumentów. Komisja powołała też

[21] REN21 – *Renewables 2023 Global Status Report* – REN21 (Paris: REN21 Secretariat). 2023.

[22] European Commission (2022) – *Digitalising the energy system – EU Action Plan*, Komunikat COM(2022) 552 final, Brussels, 2022.

specjalną Grupę Ekspercką ds. Inteligentnej Energii (Smart Energy Expert Group) z udziałem przedstawicieli państw członkowskich, by koordynować te wysiłki.

Na poziomie krajowym w Europie widać zróżnicowanie. Niemcy – posiadające największą moc PV w UE – w 2022 r. przyjęły pakiet reform ("Osterpaket") przyspieszający rozwój OZE, w którym znalazły się zapisy o modernizacji sieci i inteligentnych rozwiązaniach (m.in. zniesienie podatku VAT na małe PV i obowiązek instalowania inteligentnych liczników). Francja i Hiszpania kładą nacisk na rozwój magazynów energii i pojazdów elektrycznych w sieci, co ściśle łączy się z AI (np. sterowanie ładowaniem EV w godzinach nadmiaru energii słonecznej). Polityki innowacji w wielu krajach UE (np. Francja AI for Humanity, Strategia AI Polski 2019) wymieniają sektor energetyczny jako priorytetowy obszar wdrożeń AI, choć często brak konkretnych mechanizmów wcielenia tego w życie. Najlepszą praktyką UE jest zapewne jej podejście regulacyjne i holistyczna strategia. UE jako jedna z nielicznych wyraźnie wskazuje w dokumentach strategicznych, że AI w energetyce może służyć zarówno równoważności, jak i bezpieczeństwu. Wspomniany plan cyfryzacji postuluje tworzenie cyfrowych bliźniaków systemu elektroenergetycznego, większą wymianę danych między operatorami sieci a producentami OZE, a także włącza sektor energii w szersze inicjatywy cyfrowe (np. chmurę europejską). Uzupełnieniem jest unijny Fundusz Odbudowy (Next Generation EU), z którego miliardy euro kierowane są na inteligentne sieci i innowacje smart grid w państwach członkowskich. Dzięki temu kraje takie jak Hiszpania czy Grecja finansują modernizację sieci przesyłowych, instalację sensorów i automatyki – przygotowując grunt pod AI. Wciąż jednak istnieją luki. UE nie posiada jednej, dedykowanej strategii łączącej AI + PV + bezpieczeństwo energetyczne – elementy te są porozrzucane w różnych politykach (AI Act, Zielony Ład, Unia Energetyczna). W praktyce implementacja zależy od państw członkowskich. Część krajów (np. Polska) szybko zwiększyła moc PV, ale cyfryzacja sieci za tym nie nadąża – co skutkuje lokalnymi problemami (przeciążenia linii, wyłączanie farm w słoneczne dni). Wyzwaniem pozostaje ujednolicenie standardów – np. interoperacyjność inteligentnych urządzeń, bezpieczeństwo danych pomiarowych – nad czym UE dopiero pracuje (zob. energy.ec.europa.eu). Niemniej, UE wydaje się świadoma konieczności aktualizacji paradygmatów bezpieczeństwa energetycznego: cyfryzacja i AI są traktowane jako nowe narzędzia zapewnienia bezpieczeństwa dostaw w epoce odnawialnej.

Chiny to światowy potentat fotowoltaiki – zainstalowana moc PV w Państwie Środka przekroczyła 392 GW na koniec 2022 r., co stanowi około 1/3 łącznej mocy fotowoltaicznej świata[23]. Żaden inny kraj nie przyłącza tyle nowych mocy słonecznych co Chiny; w 2023 r. tempo to jeszcze przyspieszyło (prognozowane dodatki rzędu 100–120 GW rocznie). Z tak ogromną bazą OZE kwestie integracji z siecią i stabilności dostaw nabierają pierwszorzędnego znaczenia. Jak zatem Chiny radzą sobie z połączeniem PV i AI? Oficjalne dokumenty strategiczne Chin dotyczące energii dotychczas nie eksponowały roli AI w kontekście bezpieczeństwa energetycznego – koncentrując się raczej na rozbudowie mocy i infrastrukturze fizycznej. Chińska strategia energetyczna (np. plan pięcioletni na lata 2021–2025) zakłada masową ekspansję OZE oraz budowę tzw. Nowego Systemu Energetycznego, obejmującego rozproszoną generację i magazyny. W tych planach wspomina się o "inteligentnych sieciach" i "internet+energia", jednak bez szczegółów. Natomiast polityka rozwoju AI w Chinach – niezwykle ambitna (Chiny chcą być globalnym liderem AI do 2030 r.) – jest traktowana jako odrębny nurt. Rząd Chiński wydał szereg wytycznych dot. AI (np. plan rozwoju AI 2017, regulacje 2022 dot. algorytmów rekomendacyjnych, 2023 dot. generatywnej AI), lecz skupiają się one na przemyśle, usługach, bezpieczeństwie publicznym, a mało bezpośrednio na energetyce. Sfera regulacyjna to jedno, ale praktyka to drugie. Chiny de facto bardzo intensywnie wdrażają AI w sektorze elektroenergetycznym, co może wynikać z olbrzymiej skali ich sieci i konieczności zarządzania nią w czasie rzeczywistym. Przykładem jest rozwój inteligentnych centrów sterowania siecią przez Państwową Sieć Energetyczną (State Grid) – operator sieci przesyłowej ChRL chwali się zastosowaniem algorytmów optymalizacyjnych do bilansowania obciążenia między regionami, co jest kluczowe, gdy na zachodzie kraju świeci słońce (ogromne farmy PV w Sinciangu i Gobi), a centra zużycia na wschodzie zgłaszają zapotrzebowanie. Ponadto Chiny inwestują w magazyny energii (w 2022 ogłoszono plan dodania 30 GW magazynów do 2025 r.) oraz elektrownie szczytowo-pompowe, które sprzężone z AI mogą buforować wahania produkcji PV. Rząd uruchomił też programy pilotażowe tzw. "energetycznego internetu rzeczy" – w wybranych miastach i prowincjach testuje się integrację tysięcy mikroźródeł, magazynów, ładowarek EV, sterowanych przez platformy AI w modelu podobnym do wirtualnej elektrowni.

[23] Reuters (2023) – Bose, S., *China's solar capacity expected to hit 1,000 GW by 2026, Rystad Energy says*, Reuters, 2023.

Co do oficjalnych inicjatyw, warto odnotować, że w marcu 2023 powołano w Chinach nowy Komitet ds. Transformacji Energetycznej (pod przewodnictwem premiera), który w agendzie ma m.in. promowanie inteligentnego podejmowania decyzji w elektroenergetyce z wykorzystaniem AI. Sugeruje to, że najwyższe kierownictwo dostrzega potrzebę połączenia tych dziedzin. Najlepszą praktyką Chin jest zatem ogromna skala wdrożeń pilotowych – np. projekty typu smart city, (w których AI zarządza lokalną siecią energetyczną z PV na dachach, magazynami i konsumentami). Azerbejdżan, aspirujący do korzystania z chińskich doświadczeń, wskazuje, że w Chinach powstają już fabryki i całe osiedla zeroemisyjne, gdzie AI monitoruje dane w czasie rzeczywistym i optymalizuje zużycie energii – co pozwala redukować emisje i poprawiać efektywność. Analiza dla Chin sugeruje, że rozwój sztucznej inteligencji przekłada się na szybszy rozwój OZE i transformację energetyczną państwa[24]. Luki w strategii Chin to przede wszystkim rozdźwięk między regulacją AI a energetyką. Silne restrykcje dotyczące np. algorytmów (prawo z 2022 wymaga rejestracji algorytmów rekomendacji) mogą hamować innowacje także w energetyce, jeśli potraktuje się je literalnie. Ponadto chińska sieć wciąż opiera się na scentralizowanym modelu zarządzania – pytanie, na ile dopuszczą oni model zdecentralizowany (prosumentów z AI), który mógłby zwiększyć bezpieczeństwo poprzez redundancję. Wyzwanie stanowi też cyberbezpieczeństwo – Chiny inwestują w technologie informatyczne w energetyce (np. własne systemy SCADA, AI oparte na krajowych chipach), by uniezależnić się od Zachodu i zabezpieczyć przed cyberatakami. Można więc uznać, że integracja PV+AI jest w Chinach faktycznie realizowana, ale strategiczny dyskurs dopiero się rozwija. W nadchodzących latach zapewne pojawią się oficjalne wytyczne wiążące AI z bezpieczeństwem sieci – być może w kolejnej pięciolatce.

Inne wybrane przykłady

Poza wyżej omówionymi głównymi graczami warto spojrzeć na kilka innych państw, gdzie integracja fotowoltaiki i AI przykuwa uwagę[25]:

- **Indie** – posiadające ok. 79 GW PV (2022) – stawiają na rozwój OZE dla poprawy bezpieczeństwa energetycznego (uniezależnienie od importu

[24] P. Zhang, L. Wei, R. Sun, *Assessing the impact of artificial intelligence on China's energy transition: A quantitative approach*. Energy Economics, 129, 105835, 2024.

[25] REN21 – *Renewables 2023 Global Status Report* – REN21 (Paris: REN21 Secretariat). 2023.

paliw). Indyjskie inicjatywy Smart Grid Mission oraz liczne startupy AI (np. w Bangalore) skutkują projektami takimi jak inteligentne mikrosieci z PV dla wsi i miast. Politycznie Indie przyjmują jednak ostrożne podejście – w strategiach częściej mówią o „cyfryzacji sektora energii", niż konkretnie AI. Trwają pilotaże sieci samobilansujących się z PV i bateriami, co ma znaczenie np. dla armii (bazy off-grid).

- **Japonia** – około 84,5 GW PV (2022) – już od lat 90. rozwija koncepcje inteligentnych domów i budynków z OZE. Japońska strategia energetyczna kładzie nacisk na niezawodność (lekcje po Fukushimie), stąd duże zainteresowanie AI w systemach obrony przed blackoutami. Powstają systemy wykorzystujące uczenie maszynowe do wczesnego wykrywania niestabilności sieci na wyspach z dużym udziałem PV i automatycznego przełączania na tryb wyspowy z lokalnymi źródłami.
- **Australia** – ciekawy przypadek kraju o ogromnym potencjale PV (największy udział PV per capita na świecie, ponad 1/4 domów z panelami). Ze względu na rozległość sieci, Australia stała się poligonem dla rozwiązań VPP – np. program South Australia VPP łączy tysiące domowych instalacji wirtualnie. AI jest kluczem do koordynacji tych zasobów. Australijska polityka skupia się na market-driven solutions, wspierając regulatoryjnie możliwość agregacji i handlu energią przez prosumentów (peer-to-peer energy trading), co de facto promuje wykorzystanie AI (bo tylko algorytmy mogą obsłużyć, tak złożony rynek, w czasie rzeczywistym).
- **Bliski Wschód (np. ZEA)** – Zjednoczone Emiraty Arabskie i Arabia Saudyjska inwestują w giga-projekty solarne (jak park Mohammed bin Rashid Al Maktoum Solar Park) oraz aspirują do roli innowatorów AI (np. saudyjska inicjatywa NEOM). W ich strategiach bezpieczeństwa energetycznego AI pojawia się w kontekście efektywności – np. redukcji strat, optymalizacji odsalania wody zasilanego PV, czy zarządzania popytem w miastach klimatyzowanych. W 2023 r. Arabia Saudyjska ogłosiła program budowy smart grid z AI w ramach Vision 2030, co ma m.in. poprawić niezawodność dostaw przy rosnącym udziale PV w miksie (aktualnie nadal dominacja ropy/gazu).

Powyższe przykłady uzupełniają obraz: na całym świecie trwają eksperymenty i wdrożenia PV+AI, natomiast ich odzwierciedlenie w oficjalnych strategiach jest różne. Tabela 1 zbiera porównanie kilku kluczowych wskaźników (moc PV, ramy polityczne AI/energia) dla wybranych graczy.

Tabela 1. Moc zainstalowana fotowoltaiki i uwzględnienie AI w strategiach – wybrane państwa (2022/2023)

Państwo/ region	Moc zainst. PV (GW) – rok 2022[1]	Udział w globalnej mocy PV[1]	Strategie AI w energetyce (stany na 2024)
Chiny	392 GW	ok. 33%	Brak osobnej strategii AI-energia; regulacje AI ogólne (2022–23) nie dedykowane sektorowi energii. De facto masowe wdrożenia smart grid i VPP; 2023 – zalecenia rządowe dot. "inteligentnej elektroenergetyki".
USA	141,6 GW	ok. 12%	Brak wzmianki o AI w strategiach bezpieczeństwa energ. 2022; istnieje Narodowa Strategia AI 2020 (ogólnonaukowa) i programy DoE (AITO, projekty pilotażowe). 2023 – rozkaz Prezydenta integrujący AI z planowaniem sieci.
UE (27)	ok. 208 GW (w tym Niemcy 67)	ok. 17% (Niemcy 5,6%)	Strategie UE uwzględniają AI pośrednio: Akt o AI (wymogi dla AI w energii), Plan cyfryzacji energii 2022 (promuje IoT/AI), krajowe strategie AI w kilku krajach (DE, FR) wspominają energetykę. Brak jednolitej strategii PV+AI, trwają prace legislacyjne.
Indie	79 GW	ok. 6,7%	Brak formalnej strategii AI w energetyce; polityka OZE zakłada inteligentne sieci. Powstaje kilka projektów smart grid z AI (np. sterowanie mikrogridami na obszarach wiejskich). Rządowe instytuty testują AI do prognoz monsunów dla PV.
Japonia	84,5 GW	ok. 7,1%	Strategia energetyczna akcentuje niezawodność – AI wykorzystywana do stabilizacji sieci (nie formalizowane w polityce). Krajowa strategia AI (2019) – sektor energii jako jeden z priorytetów R&D. Programy pilotażowe inteligentnych miast i domów z PV (society 5.0).
Australia	26,9 GW (rozdrobnione prosum.)	ok. 2,3% (ale #1 per capita)	Brak scentralizowanej polityki (kompetencja stanów); praktyka: liczne wirtualne elektrownie i systemy zarządzania popytem z AI (największa penetracja na świecie). Federalnie: finansowanie badań smart grid, brak ograniczeń regulacyjnych dla AI.

Źródło: opracowanie własne.

Wyzwania integracji PV+AI

Mimo obiecujących korzyści, integracja fotowoltaiki i AI nie jest wolna od wyzwań. Identyfikacja tych barier ma kluczowe znaczenie, by strategie bezpieczeństwa energetycznego były kompletne i realistyczne. Poniżej omówiono najważniejsze z nich:

1) **Cyberbezpieczeństwo i odporność systemu.** Wraz z rosnącą cyfryzacją infrastruktury energetycznej pojawia się istotne ryzyko ataków cybernetycznych i nieautoryzowanych ingerencji. Paradoksalnie, coś co ma zwiększać bezpieczeństwo (AI zarządzająca siecią), może stać się nowym wektorem ataku. Inteligentne falowniki PV, liczniki smart czy koncentratory danych – jeśli zostaną zhakowane – mogą posłużyć do zakłócenia pracy systemu na dużą skalę. Raport RAND podkreśla, że podwyższone ryzyko cyber to jedno z głównych wyzwań wdrażania AI w system elektroenergetyczny[26]. Ponadto algorytmy AI bywają nieprzejrzyste (tzw. black box) – ich nieprzewidywalne działanie lub błędne decyzje również stanowią zagrożenie, zwłaszcza gdy AI autonomicznie steruje krytycznymi urządzeniami. Przykładowo, źle przeszkolony agent AI mógłby w niewłaściwym momencie odłączyć magazyn energii, potęgując awarię zamiast jej zapobiec. Aby zyskać zaufanie do AI, regulatorzy muszą wprowadzić normy i certyfikacje dla algorytmów w energetyce (co czyni UE w AI Act)[27] . Z punktu widzenia strategii państwa istotne jest też unikanie jednego dostawcy technologii (vendor lock-in) – poleganie np. tylko na zagranicznych platformach AI mogłoby tworzyć nową zależność (jak dawniej, od ropy). Podsumowując, wyzwaniem jest zapewnienie, że rozwój PV+AI idzie w parze z adekwatnymi zabezpieczeniami i ciągłym monitoringiem ryzyka.
2) **Ramy regulacyjne i standardy.** Nowe technologie często wyprzedzają prawo – tak jest i w tym przypadku. Wiele krajów nie posiada jeszcze regulacji obejmujących specyfikę AI w energetyce. Często AI wchodzi w lukę między sektorami: prawo energetyczne reguluje koncesje, moce i infrastrukturę, prawo cyfrowe – dane i algorytmy, ale brakuje spójności na styku. Przykładowo, kto ponosi odpowiedzialność, gdy algorytm zarządzający farmą PV popełni błąd skutkujący awarią sieci? Czy operator może podejmować decyzje na podstawie "czarnej skrzynki" AI bez wyjaśnień? Polityki i strategie muszą uaktualnić definicje bezpieczeństwa energetycznego, by obejmowały również aspekty cyfrowe. Dobrym kierunkiem jest tu praca UE – przegląd istniejących regulacji, czy

[26] RAND – Nouwens, Meiser et al., *The use of AI for improving energy security: Exploring risks and opportunities in the electricity system*, RAND Corporation Research Report RRA2907-1, 2024.

[27] European Commission (2022) – *Digitalising the energy system – EU Action Plan*, Komunikat COM(2022) 552 final, Brussels, 2022.

obejmują AI w energetyce i w razie potrzeby ich dostosowanie[27]. Bez ustanowienia standardów wymiany danych, interoperacyjności urządzeń IoT, czy minimalnych wymogów dla systemów wsparcia decyzji, integracja PV+AI może napotykać bariery biurokratyczne lub technologiczne. Brakujące ogniwo to także modele rynku – obecne rynki energii nie zawsze wynagradzają usługi, jakie może dać AI (np. redukcja popytu u prosumenta). Stąd część korzyści pozostaje niezdyskontowana ekonomicznie.

3) **Koszty wdrożenia i kompetencje.** Chociaż koszty samych instalacji PV spadły drastycznie, to dodanie do nich zaawansowanej automatyki, czujników, połączeń komunikacyjnych i infrastruktury IT wymaga inwestycji. Dla krajów rozwijających się może to być poważna przeszkoda – o ile panele mogą kupić tanio z Chin, o tyle wdrożenie skomplikowanych systemów AI może przekraczać ich możliwości finansowe lub organizacyjne. Potrzebne są kadry i know-how: analitycy danych, inżynierowie AI, operatorzy potrafiący korzystać z nowych narzędzi. Istnieje ryzyko, że nierówny dostęp do tych zasobów pogłębi cyfrową nierówność energetyczną między krajami bogatymi a biedniejszymi. W strategiach należałoby przewidzieć komponenty szkoleniowe i rozwojowe – tak, by bezpieczeństwo energetyczne wzmacniać budową rodzimego potencjału technologicznego. Niemniej ważna jest akceptacja społeczna: użytkownicy muszą ufać inteligentnym systemom (np. że ich dane zużycia są bezpieczne, a automatyczne sterowanie urządzeniami domowymi nie naruszy ich komfortu). Politycy powinni prowadzić dialog z obywatelami o korzyściach i zabezpieczeniach AI – w przeciwnym razie można napotkać opór, podobny do tego wobec liczników smart metering, w niektórych krajach.
4) **Obciążenie energetyczne AI.** Warto zauważyć, że AI sama w sobie zużywa energię – centra danych, serwery obsługujące uczenie maszynowe mają swój ślad energetyczny. Szacunki IEA wskazują, że globalne centra danych (w dużej mierze napędzane wzrostem AI) konsumują ok. 1% światowej elektryczności, a udział ten rośnie. Jeśli nie będzie on zasilany czystą energią, paradoksalnie AI może zwiększać popyt na prąd i obciążać system. Scenariusze przewidują, że do 2030 r. zużycie prądu przez

infrastrukturę AI może wzrosnąć o kilkadziesiąt procent[28]. To rodzi pytania o neutralność klimatyczną AI. W strategiach należałoby uwzględnić, że „nie ma AI bez energii" i planować zaopatrzenie cyfrowej gospodarki w czyste źródła (tu PV także może pomóc, zasilając np. farmy serwerów). W skali mikro, operatorzy powinni ocenić bilans – ile dodatkowego zużycia generuje u nich wdrożenie AI vs., ile oszczędza czy optymalizuje. Bez takiej oceny można wpaść w efekt odbicia: poprawa efektywności dzięki AI obniży koszty, co zachęci do większej konsumpcji energii gdzie indziej.

5) **Integracja międzysektorowa i złożoność systemu.** Bezpieczeństwo energetyczne to dziś szeroki koncept – obejmuje nie tylko prąd, ale i ciepło, paliwa, transport. AI może umożliwić tzw. sektor coupling – łączenie sektorów przez energię elektryczną (np. używanie nadwyżek PV do ładowania EV czy pomp ciepła)[28]. To wielka szansa, ale i wyzwanie: system staje się coraz bardziej skomplikowany, a ryzyko przenosi się między sektorami (np. awaria sieci prądu blokuje transport EV). Strategie muszą ogarniać tę całość. AI może wspomóc zarządzanie takim zintegrowanym systemem (np. dając priorytet krytycznym odbiorcom w sytuacji niedoborów), ale rodzi to pytania etyczne i społeczne – według jakich kryteriów algorytm ma decydować, komu odciąć dostawy w kryzysie? To dylematy, które dotychczas rozstrzygali ludzie (rządy, operatorzy) – czy powinniśmy je delegować AI? Bez społecznego konsensusu i odpowiednich regulacji może to być trudne do wdrożenia, mimo, że technicznie wykonalne.

Biorąc pod uwagę powyższe analizy, można sformułować szereg rekomendacji polityczno-strategicznych dla decydentów na szczeblu krajowym i międzynarodowym, aby efektywnie i bezpiecznie zintegrować fotowoltaikę wspieraną AI z strategiami bezpieczeństwa energetycznego[29]:

1) Włączenie AI do definicji i oceny bezpieczeństwa energetycznego. Rządy powinny formalnie uznać, że cyfrowe innowacje (AI, IoT, big data) stały się integralnym elementem infrastruktury energetycznej. Nowelizacje strategii bezpieczeństwa energetycznego powinny zawierać rozdziały poświęcone roli cyfryzacji w zapewnianiu bezpieczeństwa dostaw.

[28] WEF (2025) – Al-Zu'bi, I., *Energy and AI: the power couple that could usher in a net-zero world*, World Economic Forum, 2025.

[29] M. S. Danish, T. Senjyu, *Policy frameworks for AI-driven energy transition: Challenges and opportunities*. Sustainability, 15(14), 10612. 2023.

2) Tworzenie spójnych ram regulacyjnych dla AI w energetyce. Konieczne jest uzupełnienie istniejących przepisów tak, by pokryły lukę na styku AI-energetyka. W praktyce oznacza to np. wydanie przez regulatorów sektorowych wytycznych dla operatorów sieci odnośnie do stosowania algorytmów AI (wymogi testów bezpieczeństwa, audytu algorytmów, planów awaryjnych na wypadek błędów AI).
3) Inwestycje w infrastrukturę cyfrową i kompetencje. Decydenci powinni zapewnić odpowiednie finansowanie i zachęty dla modernizacji sieci energetycznych pod kątem zdolności do integracji PV+AI. Oznacza to wspieranie wdrożeń inteligentnych sieci (smart grid) – np. poprzez mechanizmy regulacyjne pozwalające operatorom odzyskiwać nakłady na ICT w taryfach.
4) Zapewnienie cyberbezpieczeństwa i odporności. Rządy muszą traktować kwestie cyber zagrożeń w energetyce priorytetowo. Zaleca się ustanowienie stałych mechanizmów współpracy między służbami cyberbezpieczeństwa a operatorami energii (np. wyspecjalizowane CERT dla sektora energii).
5) Tworzenie zachęt rynkowych do wykorzystania potencjału PV+AI. Rekomenduje się, by regulując rynki energii wprowadzać mechanizmy wynagradzające usługi elastyczności i stabilizacji świadczone przez rozproszone zasoby sterowane AI.

Podsumowanie

Fotowoltaika wspierana sztuczną inteligencją jawi się jako nieodzowny element przyszłych strategii bezpieczeństwa energetycznego[30]. Analiza globalnych trendów pokazała, że rosnący udział energii słonecznej w miksie wymusza nowatorskie podejścia do zarządzania systemem – i tu AI oferuje narzędzia pozwalające zachować stabilność i niezawodność dostaw. Państwa takie jak USA, Chiny czy członkowie UE już wdrażają rozwiązania PV+AI, choć stopień formalnego uwzględnienia ich w strategiach jest różny. Najlepsze praktyki obejmują m.in. inwestycje w inteligentne sieci (UE), tworzenie instytucjonalnych ram dla AI (USA – biuro AITO, rozkazy prezydenckie) czy masowe pilotaże technologii (Chiny). Z drugiej strony, luki strategiczne są widoczne tam, gdzie polityki bezpieczeństwa energetycznego nie nadążają za

[30] J. Xiao, F. Nadeem, M. Velli, Balancing energy security, decarbonization, and economic growth: The pivotal role of AI-based PV solutions, Applied Energy, t. 348, 121474, 2024.

technologiczną rzeczywistością – przykładowo brak wzmianek o AI w kluczowych dokumentach, brak standardów bezpieczeństwa czy niepełne wykorzystanie potencjału danych. W perspektywie globalnej, aby w pełni wykorzystać synergię fotowoltaiki i AI, konieczna jest aktualizacja paradygmatów polityki energetycznej. Bezpieczeństwo energetyczne w epoce transformacji, to nie tylko kwestia posiadania surowców czy mocy wytwórczych, ale też umiejętnego zarządzania informacją i technologią. Państwa, które szybko się do tego dostosują, zyskają przewagę – będą mogły bezpiecznie integrować duże wolumeny OZE, zapewniając jednocześnie stabilne i tanie dostawy energii swoim obywatelom. Z kolei opóźnienia lub zaniedbania (np. brak zabezpieczeń cybernetycznych) mogą prowadzić do nowych rodzajów kryzysów energetycznych. Podsumowując, fotowoltaika wspierana sztuczną inteligencją, to nie pieśń przyszłości, lecz już kształtująca się rzeczywistość.



Rysunek 2. Schemat koncepcji inteligentnej sieci integrującej źródła OZE (fotowoltaika, wiatr) z odbiorcami (domy, pojazdy elektryczne, przemysł) za pomocą strategii sterowania opartych na AI

Źródło: Zulu, M.L.T., Carpanen, R.P., Tiako, R., *A Comprehensive Review: AI Optimization in a Hybrid Microgrid under Faults*, Energies, 16(4), 1786, 2023.

Rysunek 2 obrazuje taką przyszłościową wizję – inteligentny system energetyczny, gdzie słońce, wiatr, magazyny, pojazdy i budynki połączone są siecią AI control strategies, niczym mózgiem operacji. Taka integracja przynosi

liczne korzyści: więcej czystej energii w systemie, większa elastyczność i efektywność, nowe usługi dla prosumentów, a ostatecznie – wzmocnione bezpieczeństwo energetyczne rozumiane jako zdolność do zaspokojenia potrzeb energetycznych w każdych warunkach. Warunkiem jest jednak, by decydenci dziś odpowiednio pokierowali strategiami, tworząc dogodne warunki dla bezpiecznego rozwoju tych technologii. Państwa, które zaniedbają ten obszar, mogą nie tylko stracić szansę na przyspieszenie zielonej transformacji, ale wręcz narazić się na nowe zagrożenia. Dlatego rekomendacje przedstawione powyżej powinny znaleźć odzwierciedlenie w politykach – tak, aby integracja fotowoltaiki wspieranej AI stała się filarem bezpiecznej, nowoczesnej i zrównoważonej energetyki na całym świecie.

Literatura

1. Balamurugan, R., Huang, M., Kim, D., Amano, H., *Smart Grids and Artificial Intelligence: Enabling large-scale solar and wind penetration*, Frontiers in Energy Research, t. 13, 1155337, 2025.
2. Chen, H., Park, J., Li, Q., Revolutionizing solar PV integration: AI-driven forecasting and grid stability, *Energy*, t. 263, 125879. 2025.
3. Danish, M.S., Senjyu, T., *Policy frameworks for AI-driven energy transition: Challenges and opportunities*, Sustainability, t. 15, nr 14, 10612, 2023.
4. European Commission, *Digitalising the energy system – EU Action Plan*, COM(2022) 552 final, Brussels, 2022.
5. IEA, Why *AI and energy are the new power couple*, IEA Commentary, 2023.
6. IEA, Press Release: *IEA's first major Global Conference on Energy & AI*, International Energy Agency, 2024.
7. IEA-PVPS, IEA Photovoltaic Power Systems Programme, *Snapshot of Global PV Markets 2023*, Report IEA-PVPS T1-42:2024, 2024.
8. Kyriakarakos, G., Editorial: *AI, clean energy, and the resilience of future power systems*, Sustainability, t. 17, nr 3, 1987, 2025.
9. Raman, S., Kumari, S., Ortiz, A., *Synergizing AI and renewables to achieve SDG7: A global assessment of energy security and sustainability*, Sustainability, t. 16, nr 8, 4501, 2024.
10. RAND, Nouwens, Meiser et al., *The use of AI for improving energy security: Exploring risks and opportunities in the electricity system*, RAND Corporation Research Report RRA2907-1, 2024.
11. REN21, *Renewables 2023 Global Status Report*, REN21 Secretariat, Paris, 2023.
12. Reuters, Bose, S., *China's solar capacity expected to hit 1,000 GW by 2026*, Rystad Energy says, 12 Sept. 2023.
13. Tian, X., Foong, A., Nguyen, T., *Artificial Intelligence Applications in Photovoltaic Systems: A Comprehensive Review*, CAAI Artificial Intelligence Research, t. 11, nr 2, 2024, pp. 146-160.

14. Wang, Y., Zhao, X., Martin, J., Liu, S., *The role of AI in accelerating the adoption of intermittent renewable energies*, *Energy Strategy Reviews*, t. 40, 103045, 2025.
15. WEF, Al-Zu'bi, I., *Energy and AI: the power couple that could usher in a net-zero world*, World Economic Forum, 29 Jan 2025.
16. Xiao, J., Nadeem, F., Velli, M., *Balancing energy security, decarbonization, and economic growth: The pivotal role of AI-based PV solutions*, Applied Energy, t. 348, art. nr 121474, 2024.
17. Zhang, P., Wei, L., Sun, R., *Assessing the impact of artificial intelligence on China's energy transition: A quantitative approach*, Energy Economics, t. 129, 105835, 2024.
18. Zulu, M.L.T., Carpanen, R.P., Tiako, R., *A Comprehensive Review: AI Optimization in a Hybrid Microgrid under Faults*, Energies, 16(4), 1786, 2023.

prof. dr hab. n. med. i n. o zdr. Jerzy Bertrandt
Akademia Bialska im. Jana Pawła II

mgr Justyna Bandura
20 Wojskowy Szpital Uzdrowiskowo Rehabilitacyjny w Krynicy Zdroju

mgr Karolina Bertrandt-Tomaszewska
Wojskowy Instytut Medycyny Lotniczej
https://doi.org/10.29316/9788368103199_13

OTYŁOŚĆ – WSPÓŁCZESNE ZAGROŻENIE BEZPIECZEŃSTWA ZDROWOTNEGO

OBESITY – A CONTEMPORARY HEALTH SECURITY THREAT

Streszczenie

Otyłość stanowi istotny problemem zdrowia publicznego, z poważnymi konsekwencjami zdrowotnymi, które obejmują zwiększone ryzyko powstawania chorób przewlekłych, takich jak cukrzyca typu 2 i choroby układu krążenie, a także niektóre nowotwory i problemy ze zdrowiem psychicznym. Ma również negatywny wpływ na jakość życia i jego skrócenie. Aktualnie obserwujemy pandemię otyłości i jej zdrowotnych konsekwencji, co stwarza zagrożenie bezpieczeństwa zdrowotnego. W rozdziale przedstawiono definicje nadwagi i otyłości, przyczyny powstawania oraz jej zdrowotne skutki. Zwrócono uwagę na epidemiologię występowania nadwagi i otyłości na świecie i w Polsce oraz trendy

Summary

Obesity is a significant public health problem with serious health consequences, including increased risk of chronic diseases such as type 2 diabetes and cardiovascular disease, as well as some cancers and mental health problems. It also has a negative impact on the quality of life and its shortening. We are currently observing a pandemic of obesity and its health consequences, which poses a threat to health security. The chapter presents definitions of obesity and obesity, causes of development and its health effects. Attention is drawn to the epidemiology of overweight and obesity in the world and in Poland, as well as trends indicating an alarming increase in the problem among both adults and children worldwide

wskazujące na alarmujący wzrost problemu zarówno wśród dorosłych, jak i dzieci na całym świecie ze szczególnym uwzględnieniem środowiska służb mundurowych. Przedstawiono także działania podejmowane na rzecz walki z nadwagą i otyłością.

Słowa kluczowe: nadwaga i otyłość, choroby metaboliczne, służby mundurowe

and Poland, with particular emphasis on the uniformed services. Actions taken to combat overweight and obesity are also presented.

Keywords: overweight and obesity, metabolic diseases, uniformed services

Wstęp

Pandemie, zagrożenia zdrowia i niewydolność systemów opieki zdrowotnej stanowią jedne z największych zagrożeń dla światowej gospodarki i bezpieczeństwa, z jakimi przyszło się dziś mierzyć. Otyłość jest jednym z najpoważniejszych globalnych wyzwań w zakresie zdrowia publicznego w XXI wieku i jednym z najbardziej widocznych, a jednocześnie najbardziej zaniedbanych problemów zdrowotnych na świecie. W ciągu ostatnich trzech dekad wiele krajów na całym świecie odnotowało dwu- lub trzykrotny wzrost częstości występowania otyłości, prawdopodobnie z powodu urbanizacji, siedzącego trybu życia i zwiększonego spożycia wysokokalorycznej, przetworzonej żywności. Alarmujący wzrost otyłości u dzieci spowoduje w przyszłych systemach opieki zdrowotnej na całym świecie ogromne obciążenie budżetów wielu państw wynikające z konieczności stosowania profilaktyki i leczenia chorób przewlekłych.

Zapobieganie otyłości jest kluczowym czynnikiem w kontrolowaniu cywilizacyjnych chorób metabolicznych związanych z otyłością, w tym cukrzycy, chorób układu krążenia, udarów, nadciśnienia, niektórych nowotworów i problemów psychologicznych[1].

W wieku dorosłym jest ona głównym czynnikiem ryzyka złego stanu zdrowia i przedwczesnej śmierci. Także otyłość u dzieci stanowi światowy pandemiczny problem zdrowotny. Znacząco wpływa na zdrowie fizyczne i psychiczne dzieci, może prowadzić do poważnych schorzeń, w tym cukrzycy insulinoniezależnej, problemów sercowo-naczyniowych, astmy oskrzelowej, obturacyjnego bezdechu sennego, nadciśnienia, stłuszczenia wątroby, refluksu

[1] A. Tiwari, P. Balasundaram, *Public Health Considerations Regarding Obesity*, [Updated 2023 Jun 5]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK572122/, [dostęp: 08.03.2025].

żołądkowo-przełykowego i problemów psychospołecznych[2]. Biorąc pod uwagę fakt, że w 2022 roku 2,5 miliarda światowej populacji osób dorosłych w wieku 18 lat i starszych miało nadwagę, w tym ponad 890 milionów cierpiało na otyłość, należy przyjąć, że mamy do czynienia z pandemią otyłości i jej zdrowotnymi oraz gospodarczymi skutkami[3].

Rozumienie bezpieczeństwa zdrowotnego w kontekście zdrowia publicznego zostało sformułowane w Światowym Raporcie Zdrowia z 2007 roku. Światowa Organizacja Zdrowia (WHO) globalne bezpieczeństwo zdrowia publicznego definiuje jako „działania proaktywne i reaktywne podejmowane w celu zminimalizowania niebezpieczeństwa i skutków ostrych zdarzeń zagrażających zdrowiu, które zagrażają zdrowiu ludzi w różnych regionach geograficznych i granicach międzynarodowych”[4].

W świetle powyższej definicji pandemia otyłości i jej skutki stwarzają zagrożenie bezpieczeństwa zdrowotnego nie tylko w wielu krajach o wysokim wskaźniku występowania otyłości, ale także szeroko rozumianego światowego bezpieczeństwa zdrowotnego.

W Polsce, pojęcie „bezpieczeństwo zdrowotne” zostało po raz pierwszy zdefiniowane w 2014 r. w „Strategii bezpieczeństwa narodowego RP”. Dokument ten stanowił, że „bezpieczeństwo zdrowotne obywateli współkształtuje bezpieczeństwo narodowe” oraz, że wpływają na nie nasilające się zmiany demograficzne, zmiany warunków środowiskowych oraz rozwój nowych technologii”[5]. Problematykę bezpieczeństwa zdrowotnego uwzględniono także w kolejnej Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 12 maja 2020 r., w której mówi się m.in., że „w zakresie systemu ochrony zdrowia kluczowe jest przeciwdziałanie skutkom chorób cywilizacyjnych, niwelowanie społecznych nierówności w dostępie do opieki zdrowotnej i zwiększenie świadomości zdrowotnej obywateli”[6]. A przecież otyłość nie tylko generuje powstawanie wielu dietozależnych chorób cywilizacyjnych, ale już sama w sobie jest chorobą cywilizacyjną.

---

[2] P. Balasundaram, S. Krishna, *Obesity Effects on Child Health* [Updated 2023 Apr 10]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK570613, [dostęp: 09.03.2025].

[3] *Obesity and overweight*, www.who.int/news-room/fact-sheets/detail/obesity-and-overweight, [dostęp: 09.03.2025].

[4] World Health Organization: The World Health Report 2007 – A Safer Future: Global Public Health Security in the 21st Century, World Health Organization, Geneva 2007.

[5] Strategia Bezpieczeństwa Narodowego, Warszawa 2014, s. 24.

[6] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020, s. 9.

Nadmierna masa ciała i jej konsekwencje zdrowotne

Nadwaga i otyłość – charakterystyka i klasyfikacja

Światowa Organizacja Zdrowia określa nadwagę jako stan nadmiernego gromadzenia się tłuszczu, podczas gdy otyłość definiuje jako złożoną chorobę przewlekłą charakteryzującą się nadmiernym gromadzeniem się tłuszczu, która może upośledzać zdrowie[7].

Z uwagi na sposób powstawania otyłość możemy podzielić na pierwotną (prostą, pokarmową), która jest spowodowana przyjmowaniem wraz z pożywieniem nadmiernych ilości energii w stosunku do wydatku energetycznego oraz wtórną, która jest następstwem chorób lub zaburzeń, jak również może być efektem leków przyjmowanych długotrwale mn.in. przeciwdrgawkowych, sterydów, niektórych hormonów, itp.[8]

Ze względu na rozłożenie tkanki tłuszczowej w organizmie wydzielono 3 typy otyłości:

- otyłość uogólniona – charakteryzuje się rozmieszczeniem tłuszczu w całym ciele,
- otyłość androidalna (typu jabłko) – tkanka tłuszczowa gromadzi się na brzuchu - otyłość tego typu występuje głównie u mężczyzn;
- otyłość gynoidalna (typu gruszka) – tkanka tłuszczowa gromadzi się na pośladkach i udach - tego typu otyłość dotyczy częściej osób płci żeńskiej.

Otyłość androidalna może być bardziej szkodliwa niż otyłość gynoidalna, ponieważ wiąże się z większym ryzykiem wystąpienia takich schorzeń, jak choroby serca, wysokie ciśnienie krwi, bezdech senny, cukrzyca, niektóre nowotwory i udar. Wykazano, że u osób starszych otyłość androidalna, w porównaniu do otyłości gynoidalnej w większym stopniu predysponuje do powstawania zespołu metabolicznego, a także wiąże się insulinoopornością i cukrzycą, podczas gdy gromadzenie się tłuszczu w okolicach pośladkowo-udowych (otyłość gynoidalna) jest związane z korzystniejszym profilem lipidowym i glikemicznym oraz ze zmniejszeniem częstości występowania chorób sercowo-naczyniowych i metabolicznych. Badania przeprowadzone

[7] *Obesity and overweight*, www.who.int/news-room/fact-sheets/detail/obesity-and-overweight, [dostęp: 04.03.2025].

[8] P. Suchodolska, A. Orkusz, *Otyłość – przyczyny, rodzaje, leczenie, skutki. nauki inżynierskie i technologie*, Nauki Inżynierskie i Technologie, 4(31), 2018, s. 65-79.

na młodszych populacjach wykazały również, że otyłość brzuszna jest ściślej powiązana z czynnikami ryzyka metabolicznego[9].

Istnieją różne metody badania otyłości, a najpowszechniej stosowaną metodą jest wskaźnik masy ciała (BMI).

Zaburzenia masy ciała człowieka najczęściej diagnozuje się w oparciu o wartości wskaźnika masy ciała (Body Mass Index - BMI), który stanowi stosunek kwadratu wzrostu (m) do masy ciała (kg). U dorosłych wartość BMI powyżej 25 jest uważana za nadwagę, a powyżej 30 za otyłość. U dzieci w wieku 5–19 lat nadwagą jest wartość BMI dla danego wieku większa niż 1 odchylenie standardowe powyżej mediany w odniesieniu wzrostu, a otyłość, gdy wartość BMI jest większa niż 2 odchylenia standardowe. Wskaźnik masy ciała jest zastępczym wskaźnikiem otłuszczenia, przy czym w rozpoznaniu otyłości mogą pomóc dodatkowe pomiary, takie jak np. obwodu talii, czy też zawartości tkanki tłuszczowej[10].

W raporcie ekspertów Światowej Organizacji Zdrowia zaproponowano kryteria zaburzeń masy ciała stosownie do wartości BMI, które odzwierciedlają rosnące ryzyko nadwagi w miarę wzrostu BMI powyżej optymalnego zakresu 21–23 kg/m², czyli zalecanego średniego celu dla dorosłych osób rasy białej[11]. Klasyfikację nadmiernej masy ciała ilustruje tabela 1.

Tabela 1. Klasyfikacja nadwagi i otyłości

Klasyfikacja	Wartość BMI (kg/m²)
Prawidłowa masa ciała	18,5 – 24,99
Nadwaga w tym otyłość	>25,0
Otyłość	>30,0
Otyłość olbrzymia	>40,0

Źródło: Obesity classification, www.worldobesity.org/about/about-obesity/obesity-classification, [dostęp: 14.03.2025].

Ocena BMI jest prostym pomiarem, który jest bardzo przydatny dla badań populacji. Na podstawie tego pomiaru można przewidywać ryzyko u jednostek. W końcu BMI jest miarą wielkości, a nie zdrowia, więc ma pewne

[9] C. I. Sari, N. Eikelis, G. A. Head, M. Schlaich, P. Meikle, G. Lambert, E. Lambert, *Android fat deposition and its association with cardiovascular risk factors in overweight young males,* Front Physiol, 10, 1162, 2019.

[10] Obesity. www.who.int/west ernpacific/health-topics/obesity#tab=tab_1, [dostęp: 04.03.2025].

[11] *Obesity: preventing and managing. The global epidemic. Report of a WHO Consultation,* WHO Technical Report Series 894. WHO, Geneva 2000.

ograniczenia jako narzędzie diagnostyczne. Np. sportowcy, w oparciu o wartość BMI, są często błędnie klasyfikowani jako osoby z nadwagą lub z otyłością ze względu na dużą masę mięśniową, a nie zawartość tłuszczu. Krótko mówiąc, BMI jest najbardziej przydatny na poziomie populacji i do określania ryzyka (nie diagnozy) na poziomie jednostki.

Wprawdzie nie ma powszechnie akceptowanej definicji otyłości opartej na całkowitej zawartości tłuszczu w organizmie, to jednak większość badaczy przyjmuje zawartość tłuszczu całkowitego w organizmie >25% u mężczyzn i >30% u kobiet jako punktów odcięcia do zdefiniowania otyłości[12]. Ocenę stanu odżywienia w oparciu o odsetek zawartość tłuszczu w organizmie ilustruje tabela 2[13].

Tabela 2. Klasyfikacja otyłości w oparciu o odsetek zawartości tłuszczu w organizmie

	Norma	Nadmierna masa tłuszczu	Otyłość	Otyłość olbrzymia
Mężczyźni	10 – 20%	20 - 25%	25 – 30%	>30%
Kobiety	20 – 30%	30 – 35%	35 – 40%	>40%

Źródło: P. Deurenberg, M. Yap, W.A. Van Staveren, Body mass index as a percent body gat: a meta-analysis among different ethnic groups, Int. J. Obesity, 22, 1998, s. 1164-1171.

Inne metody klasyfikacji otyłości obejmują pomiar obwodu talii, stosunku talii do bioder i stopień zaawansowania otyłości (Edmonton Obesity Staging System - EOSS).

Obwód talii (WC) jest tanią i łatwą metodą pomiaru i jest uważany za rozsądny wskaźnik zawartości tłuszczu wewnątrzbrzusznego lub trzewnego. Tłuszcz ten jest ściśle związany ze zwiększonym ryzykiem wielu chorób metabolicznych. Obwód talii jako miara otyłości trzewnej może uzupełniać BMI w ocenie ryzyka. Otyłość brzuszna jest niezależnym czynnikiem ryzyka (nawet gdy BMI nie jest podwyższone) i jest predyktorem chorób współistniejących i śmiertelności. Wysokie ryzyko definiuje się, jeśli obwód talii jest większy 102 cm dla mężczyzn i większy niż 88 cm dla kobiet.

[12] D. O. Okorodudu, M. F. Jumean, V. M. Montori, A. Romero-Corral, V. K. Somers, P. J. Erwin, et al. (May 2010), *Diagnostic performance of body mass index to identify obesity as defined by body adiposity: a systematic review and meta-analysis,* International Journal of Obesity, 34(5), 2010, s. 791-799.

[13] P. Deurenberg, M. Yap, W. A. Van Staveren, *Body mass index as a percent body gat: a meta-analysis among different ethnic groups,* Int. J. Obesity, 22, 1998, s. 1164-1171.

Światowa Organizacja Zdrowia zidentyfikowała poziomy ryzyka łączące zarówno BMI, jak i WC. Wskaźnik talia-biodra (WHR) to prosty pomiar stosowany do oceny rozmieszczenia tkanki tłuszczowej, szczególnie tłuszczu brzusznego, poprzez podzielenie obwodu talii przez obwód bioder. Jest to prosty wskaźnik otyłości centralnej i może pomóc przewidzieć ryzyko wystąpienia różnych problemów zdrowotnych związanych z nadmiarem tłuszczu brzusznego. Otyłość brzuszna jest dalej definiowana jako wskaźnik talia-biodra powyżej 0,90 dla mężczyzn i powyżej 0,85 dla kobiet. Współczynnik ten określa, czy nadmiar masy ciała gromadzi się w talii, co powoduje zwiększone ryzyko chorób współistniejących. Kryteria wzrostu ryzyka wystąpienia zaburzeń metabolicznych w zależności od obwodu talii ilustruje tabela 3[14].

Tabela 3. Ryzyko zaburzeń metabolicznych w zależności od wartości WC i WHR

Wskaźnik	Punkty odcięcia	Ryzyko zaburzeń metabolicznych
Obwód w talii	>94 cm (M); >80 cm (K)	Zwiększone
	>102 cm (M); > 88 cm (K)	Znacznie zwiększone
Stosunek obwodu w talii do obwodu w biodrach	≥0,90 cm (M); ≥0,85 cm (K)	Znacznie zwiększone

Źródło: Waist Circumference and Waist-Hip Ratio. Report of a WHO Expert Consultation, WHO, Geneva, 8-11 December 2008.

Coraz częściej w warunkach klinicznych jest stosowana ocena stopnia zaawansowania otyłości (Edmonton Obesity Staging System - EOSS). EOSS diagnozuje i bierze pod uwagę stopień otyłości na podstawie klinicznej oceny problemów zdrowotnych związanych z wagą, zdrowiem psychicznym i jakością życia. Jest on przydatny na poziomie indywidualnym i przy podejmowaniu decyzji o leczeniu, ale nie jest praktyczny do wykorzystania na poziomie populacji[15].

Wreszcie, dostępne są również skany impedancji biometrycznej, obrazowania metodą rezonansu magnetycznego, tomografii komputerowej i absorpcjometrii rentgenowskiej o podwójnej energii, ale większość z nich jest zwykle zbyt droga, aby można było ich używać w przypadku dużych badań populacyjnych.

[14] *Waist Circumference and Waist-Hip Ratio. Report of a WHO Expert Consultation*, WHO, Geneva, 8-11 December 2008.

[15] J. Myung, K.Y. Jung, T. H. Kim, E. Han, *Assessment of the validity of multiple obesity indices compared with obesity-related co-morbidities*, Public Health Nutr, 22(7), 2019, s. 1241-1249.

Przyczyny powstawania otyłości

Istnieje wiele czynników ryzyka powstawania nadwagi i otyłości. Niektóre z nich to czynniki indywidualne, takie jak wiedza, umiejętności i zachowania. Inne znajdują się w naszym otoczeniu, takim jak szkoła, miejsce pracy i sąsiedztwo. Ponadto praktyki przemysłu spożywczego i marketing, a także normy i wartości społeczne i kulturowe mogą również wpływać na ryzyko powstawania otyłości. Otyłość może wynikać z niezdrowej diety, braku aktywności fizycznej, czynników genetycznych, hormonalnych oraz psychologicznych. Ważnym czynnikiem ryzyka są także stres i zaburzenia snu. Nadwaga i otyłość mogą się rozwinąć, gdy przez dłuższy czas przyjmujemy w ciągu doby z pożywieniem więcej energii niż wydatkujemy. Jest to również opisywane jako zaburzenie równowagi energetycznej (dobowego bilansu energetycznego). Gdy energia wejściowa (kalorie) nie jest równa energii wyjściowej (kalorie, które organizm wykorzystuje do takich czynności, jak oddychanie, trawienie pokarmu i aktywność fizyczna) mamy do czynienia z dodatnim dobowym bilansem energetycznym[16]. Nadmiar energii jest odkładany w organizmie w postaci zapasowej tkanki tłuszczowej, stanowiącej jej zapas na czas niedoborów energetycznych.

Nadwaga i otyłość- konsekwencje zdrowotne

Nadwaga i otyłość wiążą się ze zwiększonym ryzykiem wystąpienia wielu poważnych chorób i problemów zdrowotnych. Osoby, które mają nadwagę lub otyłość są, w porównaniu do osób o prawidłowej masie ciała, znacznie bardziej obarczone ryzykiem powstawania wielu chorób, określanych mianem dietozależnych, cywilizacyjnych chorób metabolicznych, a także innych schorzeń. Należą do nich: wysokie ciśnienie krwi (nadciśnienie), wysoki lub niski poziom cholesterolu LDL i wysoki poziom triacydoglicerydów (dyslipidemia), cukrzyca typu 2, choroba niedokrwienna serca, udar, kamica pęcherzyka żółciowego, choroba zwyrodnieniowa stawów, bezdech senny i problemy z oddychaniem, niektóre rodzaje nowotworów, choroby psychiczne, takie jak depresja kliniczna, lęk i inne zaburzenia psychiczne. Choroby te w istotny sposób obniżają jakość życia otyłych i stanowią przyczynę przedwczesnych zgonów lub znacznej niepełnosprawności. Przyjmuje

[16] *Overweight and Obesity*, Causes and Risk Factors, www.nhlbi.nih.gov/health/overweight-and-obesity/causes, [dostęp: 19.04.2025].

się, że ryzyko problemów zdrowotnych zaczyna się, już wtedy, gdy człowiek ma tylko niewielką nadwagę, a prawdopodobieństwo problemów wzrasta, gdy staje się coraz bardziej otyły. Niezależnie od zaburzeń stanu zdrowia osoby otyłej oraz kosztów ponoszonych przez rodzinę takiej osoby, to koszty dla systemu opieki zdrowotnej mogą być niezwykle wysokie. Jednakże nadwaga i otyłość to zaburzenia, które są w dużej mierze możliwe do uniknięcia. Kluczem do sukcesu jest osiągnięcie ustrojowej równowagi energetycznej, a więc styl życia gwarantujący utrzymanie wyrównanego bilansu energetycznego. Aby osiągnąć ten cel, należy ograniczyć spożycie energii z tłuszczów i zmienić rodzaj spożywanych tłuszczów, z tłuszczów nasyconych na tłuszcze nienasycone, zwiększyć spożycie owoców i warzyw, a także roślin strączkowych, pełnych ziaren i orzechów oraz ograniczyć spożycie cukrów. Ponadto należy zwiększyć aktywność fizyczną - do co najmniej 30 minut dziennie regularnej, umiarkowanej aktywności fizycznej[17,18].

Nadwaga i otyłość – epidemiologia

Nadwaga i otyłość na świecie

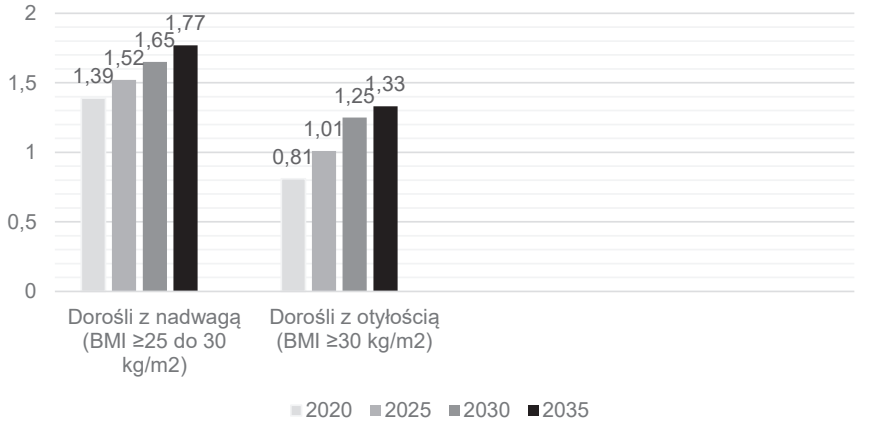
W 2022 r. jedna na osiem osób na świecie cierpiała na otyłość. Od 1990 r. na świecie otyłość dorosłych wzrosła ponad dwukrotnie, a wśród nastolatków wzrosła czterokrotnie. W 2022 r. 2,5 miliarda dorosłych w wieku 18 lat i starszych miało nadwagę. Spośród nich 890 milionów cierpiało na otyłość w tym 43% dorosłych w wieku 18 lat i starszych miało nadwagę, a 16% – otyłość. Dane WHO wskazują także, że 37 milionów dzieci poniżej 5 roku życia miało nadwagę, a ponad 390 mln dzieci i młodzieży w wieku 5–19 lat miało nadwagę, w tym 160 mln cierpiało na otyłość[19].

Analiza danych występowania nadwagi i otyłości na świecie wskazuje na wyraźne tendencje wzrastające. Prognozowaną dynamikę zmian występowania nadwagi i otyłości na świecie przedstawiono na rysunkach 1 i 2. Wysokie wartości BMI zwiększają ryzyko powstawania chorób metabolicznych.

[17] *Healthy Weight and Growth. How Overweight and Obesity Impacts Your Health*, CDC, www.cdc.gov/healthy-weight-growth/food-activity/overweight-obesity-impacts-health.html, [dostęp: 19.04.2025].

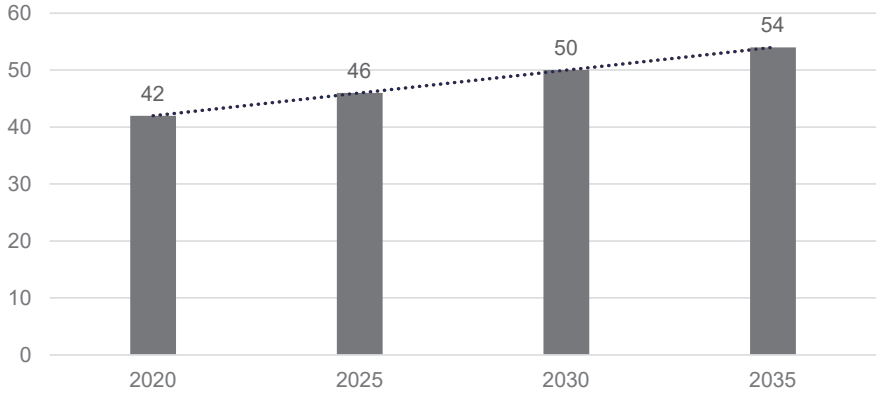
[18] *Obesity: Health consequences of being overweight*, WHO, www.who.int/news-room/questions-and-answers/item/obesity-health-consequences-of-being-overweight, 19.04.2025].

[19] *Obesity and overweight*, www.who.int/news-room/fact-sheets/detail/obesity-and-overweight, [dostęp: 04.03.2025].



Rysunek 1. Prognozowana dynamika zmian występowania nadwagi i otyłości na świecie w mld[20]

Źródło: T. Lobstein, Powis J., Jackson-Leach R. World Obesity Atlas 2024. World Obesity Federation, London 2024.



Rysunek 2. Prognozowany trend odsetka dorosłych z nadwagą i otyłością na świecie (%)

Źródło: T. Lobstein, Powis J., Jackson-Leach R. World Obesity Atlas 2024. World Obesity Federation, London 2024.

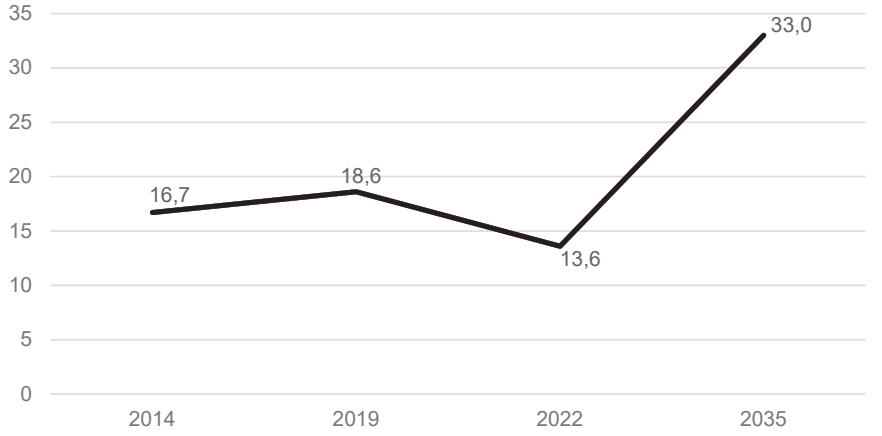
Nadwaga i otyłość w Polsce

Zgodnie ze statystykami opublikowanymi w 2021 roku przez Główny Urząd Statystyczny (GUS) w 2019 roku, w porównaniu z poprzednimi latami, w Polsce wzrósł odsetek osób z nadmierną masą ciała. W 2019 roku nadwagę

[20] T. Lobstein, J. Powis, R. Jackson-Leach, World Obesity Atlas 2024. World Obesity Federation, London 2024.

lub otyłość miało 57% dorosłych mieszkańców Polski, podczas gdy w 2014 roku nieco ponad 53%. W ciągu tych lat populacja dorosłych mężczyzn z nadwagą lub otyłością wzrosła o 3%. W 2019 roku niemal 65% ogółu mężczyzn miało nadmierną masę ciała (około 46% miało nadwagę, a niecałe 20% otyłość). Populacja dorosłych kobiet z nadwagą lub otyłością w 2019 roku także się zwiększyła o ponad 3 % w porównaniu z 2014 rokiem. Niemal 49% ogółu dorosłych kobiet miało nadmierną masę ciała (ponad 31% miało nadwagę, a niemal 18% – otyłość)[21].

W sierpniu 2022 roku Narodowy Instytut Zdrowia Publicznego PZH – Państwowy Instytut Badawczy (NIZP PZH – PIB) przeprowadził Badanie Stanu Zdrowia i Czynników Ryzyka. Wyniki pokazują, że zbyt wysoką masę ciała (indeks BMI ≥ 25) miało 52,2% Polaków w wieku 20 lat i więcej, a 13,6% cierpiało na otyłość (BMI ≥ 30). Odsetek mężczyzn z nadwagą i otyłością wynosił odpowiednio 62,1% oraz 15,7%, a w przypadku kobiet 42,6% oraz 11,7%. Rysunek 3 prezentuje podsumowanie dostępnych danych dotyczących odsetka osób z otyłością w Polsce oraz [prognozę do roku 2035][22].



Rysunek 3. Odsetek osób z otyłością w Polsce na przestrzeni lat
Źródło: opracowanie własne.

[21] I. Pawluk, P. Gosa, M. Jodkiewicz, M. Kaczorek, P. Nagel, S. Pacyna, A. Wedziuk-Reszka, K. Wolnicka, *Nadwaga i otyłość małymi krokami do zdrowia,* Narodowy Instytut Zdrowia Publicznego PZH – Państwowy Instytut Badawczy, Warszawa 2022.

[22] NFZ o zdrowiu. Otyłość i jej konsekwencje. Narodowy Fundusz Zdrowia, Warszawa 2024.

Problem dziecięcej nadwagi i otyłości stał się jednym z głównych wyzwań dla zdrowia publicznego w Polsce. W naszym kraju nadwaga lub otyłość występują u: 12,2% chłopców i 10% dziewcząt w wieku przedszkolnym oraz u 18,5% chłopców i 14,3% dziewcząt w wieku szkolnym[23]. Raport WHO wskazał, że nadwagę i otyłość odnotowano u 32% polskich dzieci w wieku 7-9 lat. Jest to 8 miejsce wśród badanych krajów w Europie. Między rokiem 2018 a 2022 wzrosła także liczba młodzieży z nadwagą i otyłością. Wyraźnie zarysowane są różnice między płciami – niezależnie od wieku nadmierną masę ciała ma około dwa razy więcej chłopców niż dziewcząt. Wraz z wiekiem spada odsetek dzieci i młodzieży z nadwagą i otyłością – u chłopców różnica ta wynosi 13 pp., u dziewcząt – 6 pp[24]. U dzieci znacznie częściej występującą, bo w 90% przypadków zachorowań, jest otyłość prosta, czyli pierwotna, będąca wynikiem długotrwałego utrzymywania się dodatniego bilansu energetycznego. Natomiast jedynie 10% przypadków otyłości stanowi otyłość wtórna, będąca wynikiem podawania leków lub objawem niektórych jednostek chorobowych[25].

Nadwaga i otyłość w służbach mundurowych

Nadwaga i otyłość, będące m.in. wynikiem wadliwego sposobu żywienia, nie tylko pogarszają samopoczucie człowieka, ale stanowią także problem zdrowotny i społeczny związany z ograniczeniem wykonywania wielu zawodów, w tym także zawodu żołnierza i funkcjonariusza.

Z problemem występowania nadwagi i otyłości mamy także do czynienia w Wojsku Polskim. Wyniki prowadzonych od wielu lat badań stanu odżywienia żołnierzy WP wykazują na stałe występowanie nadwagi i otyłości, zarówno wśród rozpoczynających służbę wojskową, jak i wśród żołnierzy zawodowych. Już prowadzone w latach 80 XX w., badania stanu odżywienia załóg okrętów Marynarki Wojennej wykazały występowanie otyłości wśród marynarzy, przy czym stwierdzono wzrost liczby otyłych wraz z czasokresem

[23] *Otyłość u dzieci – same z niej nie wyrosną,* https://pacjent.gov.pl/aktualnosc/otylosc-u-dzieci--same-z-niej-nie-wyrosna, [dostęp: 20.04.2025].

[24] L. Wiśniewska-Nogaj, *Sytuacja zdrowotna młodych Polaków: przegląd badań*, https://open.icm.edu.pl/server/api/core/bitstreams/9d4d6b61-2e8b-4087-a257-20b849e633a2/content, [dostęp: 19.04.2025].

[25] M. Pycińska, Albrecht, P., *Otyłość u dzieci*, Gastroenterologia dziecięca, Poradnik Lekarza praktyka. Pod redakcją: Albrecht, P. Wydawnictwo Czelej, Warszawa, Polska, 2014, s. 32-40.

służby[26]. W badaniach 2390 młodych mężczyzn rozpoczynających służbę wojskową w różnych rodzajach wojsk na terenie kraju stwierdzono występowanie nadwagi u 33,2% badanych, podczas gdy otyłość wykazano u 10,0%[27]. Także wyniki późniejszych badań stanu odżywienia 120 osób wojskowego personelu lotniczego wykazały występowanie nadwagi u 62,7% badanych naziemnego personelu obsługi lotów i 56,6% u personelu latającego oraz otyłości odpowiednio u 8,9% vs. 15,1%[28]. Występowanie nadwagi i w niewielkim stopniu otyłości stwierdzano także wśród żołnierzy jednostek specjalnych. Wyniki współczesnych badań stanu odżywienia żołnierzy Sił Zbrojnych RP wskazują także na występowanie nadwagi i otyłości. Wykazano, że wśród 297 badanych żołnierzy Wojsk Lądowych 63,6% miało zaburzenia stanu odżywienia o różnym stopniu nasilenia. Niepokojącym jest fakt występowania nadwagi u ponad 50% badanych oraz otyłości u prawie 10% żołnierzy. W badaniach 156 osób stanowiących załogi okrętów MW RP wykazano, że liczba marynarzy z nadwagą wzrastała wraz z wiekiem badanych, przy czym nadwagę wykazywało 49% badanych w wieku do 30 lat oraz 54,3% marynarzy w wieku do 40 lat. Otyłość obserwowano u 13,5% badanych w wieku do 30 lat i u 10,9% do 40 lat[29].

Badania stanu odżywienia funkcjonariuszy Morskiego, Nadbużańskiego oraz Bieszczadzkiego – Oddziałów Straży Granicznej (SG) przeprowadzone w ramach Narodowego Programu Zdrowia w latach 2016-2020, wykazały występowanie zaburzeń masy ciała o różnym stopniu nasilenia u ponad 60% funkcjonariuszy Morskiego Oddziału SG i u ponad 75% funkcjonariuszy w pozostałych badanych oddziałach. Ponad połowa badanych funkcjonariuszy, w każdej z badanych placówek, wykazywała nadwagę, podczas gdy otyłość stwierdzono u 7,3% badanych w Morskim oddziale SG i u 22,5% badanych

[26] J. Bertrandt, A. Kłos, E. Janda, H. Frańczuk, *Ocena stanu odżywienia marynarzy odbywających zasadniczą służbę wojskową na jednostkach pływających*, Lek Wojsk, 6(11-12), 1988, s. 692- 696.

[27] A. Kłos, J. Bertrandt, *Wpływ służby wojskowej na stan odżywienia młodych mężczyzn,* Żyw Człow Metab 2000, 27(supl): 15-18.

[28] A. Klos, B. Bertrandt, J. Bertrandt, R. Łakomy, M. Jemielniak, *Ocena stanu odżywienia białkowo-energetycznego wybranego wojskowego personelu lotniczego,* Probl Hig Epidemiol, 96(4), 2015, s. 792-79.

[29] Sprawozdanie merytoryczne z realizacji tematu NPZ „Poprawa sposobu żywienia i stanu odżywiania społeczeństwa oraz aktywności fizycznej społeczeństwa", WIHE, Warszawa 2017.

w pozostałych 2 oddziałach[30]. Biorąc pod uwagę wartość wskaźnika BMI, nadmierną masę ciała wykazano u 67% badanych, natomiast nadmierną masę tkanki tłuszczowej stwierdzono u 39% funkcjonariuszy SG[31].

W innych badaniach wykazano także wysoką częstość występowania nadwagi i/lub otyłości wśród funkcjonariuszy Policji. Badaniami oceny stanu odżywienia białkowo-energetycznego objęto łącznie 289 osób, w trym 48 funkcjonariuszek i 241 funkcjonariuszy. U ponad 65% badanych występowała nadmierna masa ciała, przy czym zaburzenia te stwierdzono u 35,4% kobiet i aż u 71,8% mężczyzn. Stosownie do kryteriów oceny stanu odżywienia, w oparciu o wartości wskaźnika BMI, nadwagę wykazano u 50,9% ogółu badanych w tym u 25,0% kobiet i 56,0% mężczyzn, podczas gdy otyłość stwierdzono u 14,9% badanych, w tym u 10,4% kobiet i 15,8% mężczyzn[32].

Wyniki badania stanu odżywienia 80 słuchaczy I roku studiów Szkoły Głównej Służby Pożarniczej wykazały występowanie nadwagi u 22% badanych[33], podczas gdy wcześniejsze badania 110 słuchaczy Szkoły Aspirantów PSP wykazały nadwagę u 20% słuchaczy[34].

Działania podejmowane na rzecz walki z nadwagą i otyłością

Nadwaga i otyłość, a także powiązane z nimi choroby niezakaźne, są w dużej mierze możliwe do zapobiegania i opanowania. Na poziomie indywidualnym ludzie mogą zmniejszyć ryzyko powstawania otyłości, podejmując

[30] Sprawozdanie merytoryczne z realizacji tematu NPZ „Poprawa sposobu żywienia i stanu odżywiania społeczeństwa oraz aktywności fizycznej społeczeństwa", WIHE, Warszawa 2018.

[31] A. Anyżewska, R. Łakomy, T. Lepionka, E. Maculewicz, E. Szarska, A. Tomczak, I. Bolczyk, J. Bertrandt, *Association between Diet, Physical Activity and Nutritional Status of Male Border Guard Officers*, Int J Environ Res Public Health, 19(9), 5305, 2022.

[32] Sprawozdanie merytoryczne z realizacji tematu NPZ „Poprawa sposobu żywienia i stanu odżywiania społeczeństwa oraz aktywności fizycznej społeczeństwa", WIHE, Warszawa 2019.

[33] A. Kłos, J. Bertrandt, W. Szymańska, I. Walecka, *Ocena stanu odżywienia studentów rozpoczynających naukę w Szkole Głównej Służby Pożarniczej w Warszawie,* (Evaluation of the nutritional status of students entering the Main School of Fire Service in Warsaw) Lek. Wojsk., 88, 2010, s. 250-254.

[34] A. Kłos, J. Bertrandt, *Ocena wydatku energetycznego, wyżywienia, bilansu energetycznego oraz stanu odżywienia słuchaczy Szkoły Aspirantów Państwowej Straży Pożarnej w Krakowie*, (ekspertyza WIHE) Warszawa 1996.

interwencje zapobiegawcze na każdym etapie życia, zaczynając od okresu przed poczęciem i kontynuując je w pierwszych latach życia. Obejmują one:

- zapewnienie odpowiedniego przyrostu masy ciała w czasie ciąży;
- praktykowanie wyłącznego karmienia piersią w pierwszych 6 miesiącach po porodzie i kontynuowanie karmienia piersią do 24 miesiąca lub dłużej;
- wspieranie zachowań dzieci w zakresie zdrowego odżywiania, aktywności fizycznej, siedzącego trybu życia i snu, niezależnie od aktualnej masy ciała;
- ograniczanie czasu spędzanego przed ekranem;
- ograniczanie spożycia słodzonych napojów i wysokoenergetycznych produktów spożywczych oraz promowanie innych zdrowych zachowań żywieniowych;
- cieszenie się zdrowym życiem (zdrowa dieta, aktywność fizyczna, długość i jakość snu, unikanie tytoniu i alkoholu, samoregulacja emocjonalna);
- ograniczanie spożycia energii z tłuszczów całkowitych i cukrów oraz zwiększanie spożycia owoców i warzyw, a także roślin strączkowych, pełnych ziaren i orzechów;
- podejmowanie regularnej aktywności fizycznej.

Lekarze powinni:

- oceniać wagę i wzrost osób korzystających z placówek służby zdrowia;
- udzielać porad dotyczących zdrowej diety i stylu życia;
- w przypadku stwierdzenia otyłości, zapewniać zintegrowane usługi zdrowotne w zakresie zapobiegania otyłości i jej leczenia, w tym dotyczące zdrowej diety, aktywności fizycznej oraz środków medycznych i
- monitorować inne czynniki ryzyka chorób niezakaźnych (poziom glukozy we krwi, lipidów i ciśnienie krwi) i oceniać obecność chorób współistniejących i niepełnosprawności, w tym zaburzeń zdrowia psychicznego.

Także przemysł spożywczy może odegrać znaczącą rolę w promowaniu zdrowej diety poprzez:

- zmniejszenie zawartości tłuszczu, cukru i soli w przetworzonej żywności;
- zapewnienie, że zdrowe i odżywcze wybory są dostępne i przystępne cenowo dla wszystkich konsumentów;
- ograniczenie marketingu żywności o wysokiej zawartości cukru, soli i tłuszczu, zwłaszcza tej przeznaczonej dla dzieci i nastolatków; oraz
- zapewnienie dostępności zdrowych wyborów żywieniowych i wspieranie regularnej aktywności fizycznej w miejscu pracy.

W zapobieganiu nadwagi i otyłości istotne jest także podejmowanie określonych działań na szczeblu państwowym związanych z kształtowaniem odpowiedniej prozdrowotnej polityki. Takie polityki i działania obejmują:

- działania strukturalne, fiskalne i regulacyjne mające na celu tworzenie zdrowego środowiska żywnościowego, które sprawia, że zdrowsze opcje żywnościowe są dostępne, osiągalne i pożądane;
- reakcje sektora zdrowia zaprojektowane i wyposażone w celu identyfikacji ryzyka, zapobiegania, leczenia i zarządzania chorobą. Działania te muszą opierać się na szerszych wysiłkach na rzecz rozwiązania chorób niezakaźnych i wzmocnienia systemów opieki zdrowotnej poprzez podejście podstawowej opieki zdrowotnej i muszą być zintegrowane z nimi[35].

Nadwaga i otyłość a bezpieczeństwo zdrowotne

Jak wynika z opublikowanych dotychczas danych, narastający problem otyłości przekłada się na negatywne konsekwencje w postaci rozwoju związanych z nią licznych powikłań oraz skrócenia oczekiwanej długości życia chorych. Poza negatywnymi skutkami otyłości, jakie ponosi chory, w tym obciążeniami w wyniku rozwoju chorób przewlekłych, dolegliwościami w zakresie układu ruchu i pogarszającą się w miarę trwania otyłości ogólną jakością życia, zwraca się również uwagę na obciążenia w przestrzeni zdrowia publicznego (rosnące wydatki związane z leczeniem otyłości i jej powikłań), a w ostatnich latach również na wpływ, jaki otyłość wywiera na środowisko naturalne (niepotrzebne koszty ekologiczne związane z nadmierną produkcją i konsumpcją żywności)[36].

Otyłość to poważne zagrożenie dla bezpieczeństwa zdrowotnego, bowiem zwiększa ryzyko wystąpienia wielu chorób przewlekłych, takich jak cukrzyca typu 2, choroby serca, niektóre nowotwory oraz problemy z układem kostnym. Może również prowadzić do obniżenia jakości życia i skrócenia

[35] *Obesity and overweight*, WHO, www.who.int/news-room/fact-sheets/detail/obesity-and-overweight, [dostęp: 19.04.2025].

[36] M. Bąk-Sosnowska, M. Białkowska, P .Bogdański, T. Chomiuk, M. Gałązka-Sobotka, M. Holecki, A. Jarosińska, M. Jezierska, P. Kamiński, K. Kłoda, M. Kręgielska-Narożna, M. Lech, A. Mamcarz, A. Mastalerz-Migas, B. Matyjaszek-Matuszek, L. Ostrowska, E. Płaczkiewicz-Jankowska, E. Stachowska, M. Stelmach-Mardas, J. Szeliga, M. Szulińska, M. Walczak, M. Wyleżoł, Zalecenia kliniczne dotyczące postępowania u chorych na otyłość 2022 – stanowisko Polskiego Towarzystwa Leczenia Otyłości. Med. Prakt. wyd. spec., 2022: s. 1-87.

jego długości. Otyłość jest przyczyną ponad 200 powikłań i chorób, które są ogromnym obciążeniem dla systemu ochrony zdrowia[37].

Nadmierna masa ciała u kobiet przyczynia się do rozwoju wielu problemów ginekologicznych. W okresie rozrodczym wpływa na zmniejszenie płodności, zwiększa ryzyko poronienia, wystąpienia wad wrodzonych płodu oraz powikłań ciąży i porodu. W wielu badaniach wykazano, że kobiety chorujące na otyłość, częściej niż kobiety z prawidłową masą ciała zmagają się z problemem niepłodności. Otyłość wiąże się również z większym ryzykiem występowania nowotworów: raka piersi, raka jajnika i raka szyjki macicy. Zwiększenie BMI silnie koreluje ze zwiększonym ryzykiem wystąpienia raka piersi. Otyłość matki przed ciążą i nadmierny przyrost masy ciała w jej trakcie mogą być przyczyną powikłań ciąży i zaburzeń rozwoju płodu.

Piętnowanie nadmiernej masy ciała – powszechne w mediach, szkołach, miejscach pracy, a nawet w placówkach opieki medycznej – może prowadzić do pogorszenia samopoczucia i zdrowia psychicznego chorych na otyłość. Skutkami stygmatyzacji mogą być m.in. obniżona jakość życia, wyższy poziom lęku, zaburzenia depresyjne, nadużywanie substancji psychoaktywnych, negatywny wizerunek własnego ciała i obniżona samoocena. Przewlekle gorsze samopoczucie i lęk przed dyskryminacją lub jej doświadczanie mogą również pogłębiać problemy somatyczne, m.in. z powodu unikania przez chorych opieki medycznej i zaniechania wizyt kontrolnych, ograniczenia wychodzenia z domu, kontynuowania niezdrowych zachowań żywieniowych, niepodejmowania aktywności fizycznej, dalszego zwiększenia masy ciała, a w konsekwencji rozwoju wielu powikłań otyłości, których leczenie może być również utrudnione[38].

Jak wynika z szacunków NIK, w 2022 r choroby związane z otyłością sprawiły, że Polacy żyją krócej średnio o ok. 4 lata w porównaniu z osobami o prawidłowej masie ciała, a na otyłość choruje ok. 9 mln dorosłych osób. Z tego powodu w ostatnim czasie leczonych było prawie 800 tys. pacjentów, którym udzielono łącznie 2,2 mln świadczeń, a wydatki bezpośrednie związane

[37] I. Kazimierska, *Otyłość to choroba, a nie defekt estetyczny,* Kurier Medyczny 02.21.

[38] M. Bąk-Sosnowska, M. Białkowska, P .Bogdański, T. Chomiuk, M. Gałązka-Sobotka, M. Holecki, A. Jarosińska, M. Jezierska, P. Kamiński, K. Kłoda, M. Kręgielska-Narożna, M. Lech, A. Mamcarz, A. Mastalerz-Migas, B. Matyjaszek-Matuszek, L. Ostrowska, E. Płaczkiewicz-Jankowska, E. Stachowska, M. Stelmach-Mardas, J. Szeliga, M. Szulińska, M. Walczak, M. Wyleżoł, Zalecenia kliniczne dotyczące postępowania u chorych na otyłość 2022 – stanowisko Polskiego Towarzystwa Leczenia Otyłości. Med. Prakt. wyd. spec., 2022: s. 1-87.

z tą chorobą sięgały 9 mld zł[39]. Koszt otyłości ponoszą rodziny otyłych osób, ale także budżet państwa (zwiększone wydatki na opiekę zdrowotną) oraz pracodawcy zatrudniający osoby otyłe.

Według Stanowiska Polskiego Towarzystwa Leczenia Otyłości nieuwzględnianie otyłości w modelu opieki zdrowotnej w Polsce - skutkuje pozbawieniem wielu chorych możliwości uzyskania skutecznej opieki, której miarą jest poprawa stanu zdrowia oraz ograniczenie ryzyka powikłań. Niewłaściwe podejście do diagnostyki i leczenia otyłości w publicznym systemie ochrony zdrowia zmusza pacjentów do poszukiwania pomocy medycznej w systemie prywatnym, co z kolei pogłębia nierówności w zdrowiu, skazując osoby o niskich dochodach na wykluczenie zdrowotne. Funkcjonujące aktualnie rozwiązania organizacyjne i finansowe w systemie Narodowego Funduszu Zdrowia (NFZ) zmuszają chorych do wędrówki po wielu placówkach i korzystania z konsultacji wielu specjalistów, których praca powinna być zintegrowana i skoordynowana w ramach jednego ośrodka.

Podsumowanie

Globalne Cele Żywieniowe Światowego Zgromadzenia Zdrowia, których zadaniem jest zapewnienie braku wzrostu nadwagi u dzieci, oraz cel jakim jest powstrzymanie wzrostu zachorowań na cukrzycę i otyłość do 2025 r., zostały poparte przez Państwa Członkowskie WHO Podczas 75. Światowego Zgromadzenia Zdrowia w 2022 r. Państwa członkowskie przyjęły nowe zalecenia dotyczące zapobiegania otyłości i jej leczenia oraz poparły plan przyspieszenia WHO mający na celu powstrzymanie otyłości[40].

Wzory dietetyczne i aktywności fizycznej poszczególnych osób są w dużej mierze wynikiem warunków środowiskowych i społecznych, które znacznie ograniczają osobisty wybór. Zatrzymanie wzrostu otyłości wymaga działań wielosektorowych, takich jak produkcja żywności, marketing i ustalanie cen oraz innych, które mają na celu zajęcie się szerszymi czynnikami determinującymi zdrowie.

---

[39] *Profilaktyka i leczenie otyłości przerosły system* (zapis konferencji prasowej), www.nik.gov.pl/aktualnosci/zdrowie/coraz-wiecej-osob-z-choroba-otylosciowa-coraz-dluzsze-kolejki.html, [dostęp: 20.04.2025].

[40] *Zmiany do Międzynarodowych Przepisów Zdrowotnych* (2005) – aktualizacja informacji (stan na listopad 2023 r.) www.gov.pl/web/zdrowie/zmiany-do-miedzynarodowych-przepisow-zdrowotnych-2005--aktualizacja-informacji-stan-na-listopad-2023-r, [dostęp: 20.04.2025].

Otyłość jest odpowiedzialnością społeczną, a nie indywidualną, a rozwiązania można znaleźć poprzez tworzenie wspierających środowisk i społeczności, które uwzględniają zdrową dietę i regularną aktywność fizyczną jako najbardziej dostępne, osiągalne i niedrogie zachowania w życiu codziennym.

Literatura

1. Anyżewska A., Łakomy R., Lepionka T., Maculewicz E., Szarska E., Tomczak A., Bolczyk I., Bertrandt J., *Association between Diet, Physical Activity and Nutritional Status of Male Border Guard Officers*, Int J Environ Res Public Health, 19(9), 5305, 2022.
2. Bąk-Sosnowska M., Białkowska M., Bogdański P., Chomiuk T., Gałązka-Sobotka M., Holecki M., Jarosińska A., Jezierska M.,Kamiński P., Kłoda K., Kręgielska-Narożna M., Lech M., Mamcarz A., Mastalerz-Migas A., Matyjaszek-Matuszek B., Ostrowska L., Płaczkiewicz-Jankowska E., Stachowska E., Stelmach-Mardas M., Szeliga J., Szulińska M., Walczak M., Wyleżoł M., *Zalecenia kliniczne dotyczące postępowania u chorych na otyłość – stanowisko Polskiego Towarzystwa Leczenia Otyłości,* Med. Prakt. wyd. spec., 2022, s. 1-87.
3. Balasundaram P, Krishna S. Obesity Effects on Child Health. [Updated 2023 Apr 10]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK570613.
4. Bertrandt J, Kłos A, Janda E, Frańczuk H., *Ocena stanu odżywienia marynarzy odbywających zasadniczą służbę wojskową na jednostkach pływających,* Lek Wojsk, 6(11-12), 1988, s. 692- 696.
5. CDC. Healthy Weight and Growth. How Overweight and Obesity Impacts Your Health, www.cdc.gov/healthy-weight-growth/food-activity/overweight-obesity-impacts-health.html
6. Deurenberg P., Yap M., Van Staveren W.A., *Body mass index as a percent body gat: a meta-analysis among different ethnic groups,* Int. J. Obesity, 22, 1998, s. 1164-1171.
7. Kazimierska I., *Otyłość to choroba, a nie defekt estetyczny,* Kurier Medyczny 02.21.
8. Kłos A, Bertrandt J. Wpływ służby wojskowej na stan odżywienia młodych mężczyzn. Żyw Człow Metab, 27(supl), 2000, s. 15-18.
9. Klos A., Bertrandt B., Bertrandt J., Łakomy R., Jemielniak M., *Ocena stanu odżywienia białkowo-energetycznego wybranego wojskowego personelu lotniczego,* Probl Hig Epidemiol, 96(4), 2015, s. 792-79.
10. Kłos A., Bertrandt J., Szymańska W., Walecka I,. *Ocena stanu odżywienia studentów rozpoczynających naukę w Szkole Głównej Służby Pożarniczej w Warszawie,* (Evaluation of the nutritional status of students entering the Main School of Fire Service in Warsaw) Lek. Wojsk., 88, 2010, s. 250-254.
11. Kłos A., Bertrandt J., *Ocena wydatku energetycznego, wyżywienia, bilansu energetycznego oraz stanu odżywienia słuchaczy Szkoły Aspirantów Państwowej Straży Pożarnej w Krakowie*, (ekspertyza WIHE) Warszawa 1996.

12. Lobstein T., Powis J., Jackson-Leach R., *World Obesity Atlas 2024*, World Obesity Federation, London 2024
13. Myung J., Jung K.Y., Kim T. H., Han E. Assessment of the validity of multiple obesity indices compared with obesity-related co-morbidities. Public Health Nutr., 22(7), 2019, s. 1241–1249.
14. NFZ o zdrowiu. Otyłość i jej konsekwencje. Narodowy Fundusz Zdrowia, Warszawa 2024.
15. Obesity and overweight. www.who.int/news-room/fact-sheets/detail/obesity-and-overweight.
16. Obesity and overweight. www.who.int/news-room/fact-sheets/detail/obesity-and-overweight.
17. Obesity and overweight. www.who.int/news-room/fact-sheets/detail/obesity-and-overweight.
18. Obesity classification. www.worldobesity.org/about/about-obesity/obesity-classification.
19. Obesity. www.who.int/west ernpacific/health-topics/obesity#tab=tab_1 [dostęp: 04.03.2025].
20. Obesity: preventing and managing. The global epidemic. Report of a WHO Consultation. WHO Technical Report Series 894. WHO, Geneva 2000
21. Okorodudu D.O., Jumean M.F., Montori V.M., Romero-Corral A., Somers V.K., Erwin P.J., et al. Diagnostic performance of body mass index to identify obesity as defined by body adiposity: a systematic review and meta-analysis. International Journal of Obesity, 34(5), 2010, s. 791-799
22. *Otyłość u dzieci – same z niej nie wyrosną*, https://pacjent.gov.pl/aktualnosc/otylosc-u-dzieci-same-z-niej-nie-wyrosna.
23. Overweight and Obesity. Causes and Risk Factors. www.nhlbi.nih.gov/health/overweight-and-obesity/causes.
24. Pawluk I., Gosa P., Jodkiewicz M., Kaczorek M., Nagel P., Pacyna S., Wedziuk-Reszka A., Wolnicka K. *Nadwaga i otyłość małymi krokami do zdrowia,* Narodowy Instytut Zdrowia Publicznego PZH – Państwowy Instytut Badawczy, Warszawa 2022.
25. *Obesity: Health consequences of being overweight*, WHO, www.who.int/news-room/questions-and-answers/item/obesity-health-consequences-of-being-overweight.
26. *Profilaktyka i leczenie otyłości przerosły system* (zapis konferencji prasowej), www.nik.gov.pl/aktualnosci/zdrowie/coraz-wiecej-osob-z-choroba-otylosciowa-coraz-dluzsze-kolejki.html.
27. Pycińska, M., Albrecht, P., *Otyłość u dzieci*, Gastroenterologia dziecięca. Poradnik lekarza praktyka. Pod redakcją: Albrecht, P. Wydawnictwo Czelej, Warszawa, Polska, 2014, s. 32-40.
28. Sari C. I., Eikelis N., Head G.A., Schlaich M., Meikle P., Lambert G., Lambert E., *Android fat deposition and its association with cardiovascular risk factors in overweight young males,* Front Physiol., 10, 2019, 1162.
29. Sprawozdanie merytoryczne z realizacji tematu NPZ „Poprawa sposobu żywienia i stanu odżywiania społeczeństwa oraz aktywności fizycznej społeczeństwa", WIHE, Warszawa 2017.

30. Sprawozdanie merytoryczne z realizacji tematu NPZ „Poprawa sposobu żywienia i stanu odżywiania społeczeństwa oraz aktywności fizycznej społeczeństwa", WIHE, Warszawa 2018.
31. Sprawozdanie merytoryczne z realizacji tematu NPZ „Poprawa sposobu żywienia i stanu odżywiania społeczeństwa oraz aktywności fizycznej społeczeństwa", WIHE, Warszawa 2019.
32. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.
33. Strategia Bezpieczeństwa Narodowego, Warszawa 2014.
34. Suchodolska P., Orkusz A., *Otyłość – przyczyny, rodzaje, leczenie, skutki. nauki inżynierskie i technologie*, 4(31), 2018, s. 65-79. https://dbc.wroc.pl/Content/102026/Suchodolska_Orkusz_Otylosc_przyczyny_ rodzaje_leczenie_skutki_2018.pdf.
35. Tiwari A, Balasundaram P., *Public Health Considerations Regarding Obesity,* [Updated 2023 Jun 5]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK572122/.
36. WHO, *Obesity and overweight*, www.who.int/news-room/fact-sheets/detail/obesity-and-overweight.
37. WHO, *Waist Circumference and Waist-Hip Ratio*, Report of a WHO Expert Consultation, Geneva, 8–11 December 2008.
38. Wiśniewska-Nogaj L., *Sytuacja zdrowotna młodych Polaków: przegląd badań*, https://open.icm.edu.pl/server/api/core/bitstreams/9d4d6b61-2e8b-4087-a257-20b849e633a2/content.
39. *World Health Organization: The World Health Report 2007 — A Safer Future,* Global Public Health Security in the 21st Century, World Health Organization, Geneva 2007.
40. *Zmiany do Międzynarodowych Przepisów Zdrowotnych* (2005) – aktualizacja informacji (stan na listopad 2023 r.) www.gov.pl/web/zdrowie/zmiany-do-miedzynarodowych-przepisow-zdrowotnych-2005--aktualizacja-informacji-stan-na-listopad-2023-r.

dr Zdzisław Małkowski
ORCID: 0009-0002-7604-0802

dr Zbigniew Skwarek
Akademia Sztuki Wojennej
ORCID: 0000-0002-9083-4695

dr Piotr Waniek
ORCID: 0000-0003-2916-1812

mgr Andrzej Skonieczny
ORCID: 0009-0008-9198-088X
https://doi.org/10.29316/9788368103199_14

ROLA ORGANIZACJI POZARZĄDOWYCH W ZAPEWNIENIU BEZPIECZEŃSTWA HUMANITARNEGO UCHODŹCOM W POLSCE

THE ROLE OF NGOS IN ENSURING HUMANITARIAN SECURITY FOR REFUGEES IN POLAND

Streszczenie

Celem badawczym niniejszego rozdziału jest analiza roli organizacji pozarządowych w zapewnianiu bezpieczeństwa humanitarnego uchodźcom w Polsce oraz ocena ich skuteczności w kontekście wyzwań finansowych, administracyjnych i politycznych. Główny problem badawczy sformułowano: W jaki sposób organizacje pozarządowe w Polsce przyczyniają się do zapewnienia bezpieczeństwa

Summary

The research objective of this chapter rozdziału is to analyze the role of non-governmental organizations in providing humanitarian security to refugees in Poland and to assess their effectiveness in the context of financial, administrative and political challenges. The main research problem was formulated: How do non-governmental organizations in Poland contribute to ensuring

humanitarnego uchodźcom i jakie bariery ograniczają skuteczność ich działań? Postawiona hipoteza zakłada, że organizacje pozarządowe pełnią kluczową rolę w systemie wsparcia uchodźców w Polsce, jednak ich skuteczność jest ograniczona przez brak stabilnego finansowania, bariery biurokratyczne oraz niewystarczającą współpracę z administracją publiczną. Pierwsza część rozdziału przedstawia organizacje pozarządowe jako kluczowych aktorów pomocy humanitarnej, omawiając ich strukturę, misję oraz zakres działań. Druga część koncentruje się na wsparciu integracyjnym i prawnym dla uchodźców, analizując działania NGO w obszarze edukacji, rynku pracy oraz doradztwa prawnego. Ostatnia część porusza główne wyzwania, z jakimi mierzą się organizacje pozarządowe oraz prezentuje rekomendacje dotyczące zwiększenia skuteczności ich działań w kontekście przyszłej polityki migracyjnej. W badaniu wykorzystano metody teoretyczne, takie jak, analiza literatury przedmiotu, raportów organizacji pozarządowych, aktów prawnych oraz opracowań naukowych dotyczących polityki migracyjnej i systemu pomocy uchodźcom w Polsce.

Słowa kluczowe: organizacje pozarządowe, uchodźcy, bezpieczeństwo humanitarne, integracja, polityka migracyjna

humanitarian security for refugees and what barriers limit the effectiveness of their activities? The hypothesis assumes that NGOs play a key role in the refugee support system in Poland, but their effectiveness is limited by the lack of stable funding, bureaucratic barriers and insufficient cooperation with public administration. The first part of the chapter presents non-governmental organizations as key actors of humanitarian aid, discussing their structure, mission and scope of activities. The second part focuses on integration and legal support for refugees, analyzing the activities of NGOs in the area of education, the labor market and legal advice. The last part discusses the main challenges faced by NGOs and presents recommendations on how to increase the effectiveness of their activities in the context of future migration policy. The study used theoretical methods, such as the analysis of the literature on the subject, reports of non-governmental organizations, legal acts and scientific studies on migration policy and the refugee assistance system in Poland.

Keywords: non-governmental organizations, refugees, humanitarian security, integration, migration policy

Wstęp

Bezpieczeństwo humanitarne stanowi jedno z kluczowych wyzwań współczesnych społeczeństw, szczególnie w kontekście narastających kryzysów migracyjnych. W ostatnich dekadach liczba osób zmuszonych do opuszczenia swoich domów z powodu konfliktów zbrojnych, prześladowań politycznych, katastrof naturalnych czy kryzysów ekonomicznych, nieustannie rośnie. Według danych organizacji międzynarodowych, takich jak Wysoki Komisarz Narodów Zjednoczonych do spraw Uchodźców (UNHCR), skala globalnych migracji osiągnęła historycznie wysoki poziom, a liczba uchodźców oraz osób wewnętrznie przesiedlonych, przekroczyła 100 milionów.

W obliczu tych wyzwań państwa i organizacje międzynarodowe muszą podejmować działania na rzecz zapewnienia bezpieczeństwa i podstawowych praw osobom zmuszonym do opuszczenia swoich krajów. Bezpieczeństwo humanitarne, rozumiane jako ochrona podstawowych praw i zapewnienie warunków umożliwiających godne życie, wykracza poza tradycyjne pojęcie bezpieczeństwa narodowego i koncentruje się na indywidualnych potrzebach jednostki. Obejmuje ono dostęp do schronienia, opieki zdrowotnej, żywności, edukacji oraz wsparcia psychologicznego i prawnego, a także ochronę przed przemocą, dyskryminacją i wykluczeniem społecznym.

Polska jako kraj graniczący zarówno z Unią Europejską, jak i obszarami niestabilnymi politycznie, odgrywa istotną rolę w procesie przyjmowania i integracji uchodźców. W ostatnich latach liczba osób szukających schronienia w Polsce znacząco wzrosła, szczególnie w wyniku konfliktu zbrojnego w Ukrainie, kryzysu migracyjnego na granicy z Białorusią oraz napływu uchodźców z Bliskiego Wschodu, Afryki i Azji Centralnej. Odpowiedzialność za zapewnienie odpowiednich warunków bytowych i bezpieczeństwa tym osobom, spoczywa nie tylko na instytucjach państwowych, ale także na organizacjach pozarządowych (NGO), które odgrywają kluczową rolę w niesieniu pomocy humanitarnej.

Celem niniejszego rozdziału jest analiza roli organizacji pozarządowych w zapewnianiu bezpieczeństwa humanitarnego uchodźcom w Polsce. Skupiono się na kluczowych aspektach ich działalności, takich jak pomoc doraźna, wsparcie integracyjne, dostęp do opieki zdrowotnej, edukacji oraz pomoc prawna. Ponadto, rozdział omawia współpracę NGO z administracją publiczną oraz organizacjami międzynarodowymi, a także wyzwania, z jakimi mierzą się te podmioty w swojej działalności.

Organizacje pozarządowe w pomocy humanitarnej

Organizacje pozarządowe w Polsce to obecnie obszerny sektor działalności[1]. Odgrywają kluczową rolę w systemie pomocy uchodźcom w Polsce, uzupełniając działania administracji publicznej i organizacji międzynarodowych. Ich działalność koncentruje się na zapewnieniu uchodźcom bezpieczeństwa humanitarnego poprzez dostarczanie pomocy doraźnej, wsparcie

[1] K. Zalewska, K. Ochyra-Żurawska, Z. Ciekanowski, *Organizacje pozarządowe w systemie bezpieczeństwa państwa*, Studia Administracji i Bezpieczeństwa, 13(13), 2022, s. 200.

integracyjne oraz ochronę praw migrantów. Wśród najważniejszych organizacji działających w Polsce można wyróżnić:

- Polską Akcję Humanitarną[2],
- Fundację Ocalenie[3],
- Caritas Polska[4],
- Helsińską Fundację Praw Człowieka[5],
- Stowarzyszenie Interwencji Prawnej[6].

Ich misja obejmuje nie tylko pomoc materialną, ale również działania edukacyjne, które mają na celu ułatwienie uchodźcom procesu adaptacji w nowym społeczeństwie.

Jednym z głównych obszarów działalności organizacji pozarządowych jest dostarczanie podstawowych środków do życia, takich jak żywność, woda, odzież i środki higieniczne[7]. W sytuacjach kryzysowych, gdy uchodźcy przybywają do Polski często bez żadnych zasobów, organizacje te zapewniają pierwszą pomoc, organizując punkty dystrybucji żywności oraz schroniska tymczasowe. Wiele z nich prowadzi także programy wsparcia finansowego dla osób, które znalazły mieszkanie, lecz nie są w stanie samodzielnie pokryć kosztów wynajmu. Roczny budżet organizacji działającej na rzecz uchodźców w 2023 r., to przeciętnie 113 tys. zł. Niemal połowa organizacji (47%) dysponowała budżetem nie większym niż 100 tys. zł, a co czwarta organizacja (21%) miała budżet większy niż 1 mln zł[8]. Współpraca NGO z lokalnymi samorządami oraz organizacjami międzynarodowymi pozwala na organizowanie długoterminowych form zakwaterowania, umożliwiając uchodźcom stabilizację życiową.

Kolejnym istotnym aspektem ich działalności jest zapewnienie dostępu do opieki zdrowotnej i wsparcia psychologicznego. Osoby uciekające z terenów objętych wojną czy represjami często wymagają natychmiastowej pomocy medycznej oraz terapii psychologicznej w związku z traumatycznymi

[2] Polska Akcja Humanitarna - Międzynarodowa organizacja charytatywna non-profit, https://www.pah.org.pl/, [dostęp: 14.03.2025].

[3] Fundacja Ocalenie, https://ocalenie.org.pl/, [dostęp: 14.03.2025].

[4] Caritas Polska, https://caritas.pl/, [dostęp: 14.03.2025].

[5] Helsińska Fundacja Praw Człowieka, https://hfhr.pl/, [dostęp: 14.03.2025].

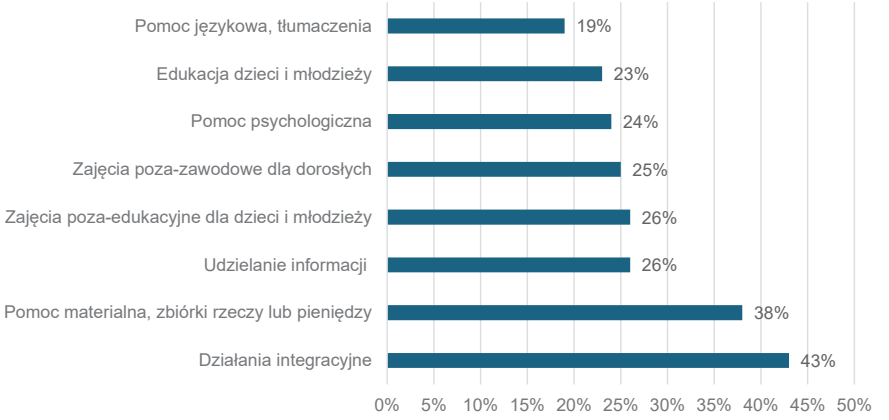
[6] Stowarzyszenie Interwencji Prawnej, https://interwencjaprawna.pl/, [dostęp: 14.03.2025].

[7] K. Jurek, *Działalność organizacji pozarządowych w kontekście kryzysu na granicy polsko-białoruskiej (2021-2022)*, Wschodnioznawstwo, nr 16, 2022, s. 134.

[8] *Kondycja organizacji pozarządowych działających na rzecz uchodźców w Polsce*, Raport z badań 2024, Stowarzyszenie klon/jawor, s. 8.

doświadczeniami[9]. Organizacje humanitarne zapewniają uchodźcom dostęp do podstawowych świadczeń zdrowotnych, leków oraz opieki psychiatrycznej, współpracując z lekarzami i placówkami medycznymi w całej Polsce. Wsparcie psychologiczne jest szczególnie istotne dla osób, które przeżyły przemoc, utratę bliskich czy długotrwałą izolację społeczną[10].

Pomoc prawna stanowi kolejny kluczowy filar działalności organizacji pozarządowych. Proces ubiegania się o status uchodźcy lub ochronę międzynarodową w Polsce jest skomplikowany i wymaga spełnienia licznych formalności. Wiele NGO oferuje bezpłatne doradztwo prawne, pomagając uchodźcom w przygotowaniu wniosków, odwołań i dokumentacji niezbędnej do legalizacji pobytu. Prawnicy współpracujący z tymi organizacjami reprezentują uchodźców przed urzędami i sądami, interweniując w przypadkach naruszeń praw człowieka czy prób deportacji. Poniżej na rysunku 1 przedstawiono rodzaje działań organizacji na rzecz uchodźców.



Rysunek 1. Rodzaje działań organizacji na rzecz uchodźców

Źródło: Kondycja organizacji pozarządowych działających na rzecz uchodźców w Polsce, Raport z badań 2024, Stowarzyszenie klon/jawor, s. 6.

Jak wynika z powyższego rysunku działania NGO obejmują również szeroko pojęte wsparcie integracyjne. Organizowane są kursy języka polskiego, szkolenia zawodowe oraz programy edukacyjne, które mają na celu

[9] K. Jasiecki, *Pomoc humanitarna dla uchodźców z Ukrainy jako katalizator nowej aktywności społecznej w Polsce*, Studia Politologiczne, nr 68, 2023, s. 139.

[10] J. Mianowski, *Dostęp imigrantek i imigrantów do systemu opieki zdrowotnej w województwie pomorskim – konstruowanie pola międzysektorowej współpracy*, Władza Sądzenia, 16, 2019, s. 105.

ułatwienie uchodźcom znalezienia pracy i dostosowanie się do polskiego rynku pracy. Szczególną uwagę poświęca się także dzieciom uchodźców, które często mają utrudniony dostęp do edukacji[11]. Organizacje pozarządowe pomagają im w adaptacji do polskiego systemu szkolnictwa, organizując zajęcia wyrównawcze oraz wsparcie psychopedagogiczne. Działania te nie tylko zwiększają szanse na samodzielne życie w Polsce, ale również przeciwdziałają marginalizacji i wykluczeniu społecznemu.

Poza świadczeniem pomocy bezpośredniej, organizacje pozarządowe pełnią również funkcję rzeczniczą, monitorując sytuację uchodźców i zwracając uwagę na systemowe problemy związane z polityką migracyjną. Poprzez raporty, kampanie społeczne i działania medialne starają się wpływać na decyzje polityczne oraz zwiększać świadomość społeczną na temat sytuacji uchodźców[12]. Ich rola w kształtowaniu debaty publicznej jest istotna, ponieważ postawy społeczne i narracja medialna mają duży wpływ na jakość życia uchodźców w Polsce.

Choć organizacje pozarządowe odgrywają nieocenioną rolę w systemie wsparcia humanitarnego, ich działalność napotyka liczne trudności. Brak stabilnego finansowania, ograniczenia biurokratyczne oraz zmieniające się regulacje prawne często utrudniają skuteczne działanie. Mimo tych wyzwań NGO nadal stanowią kluczowy filar pomocy uchodźcom w Polsce, wypełniając luki w systemie państwowym i oferując kompleksowe wsparcie zarówno w zakresie podstawowych potrzeb, jak i długoterminowej integracji.

Wsparcie integracyjne i prawne dla uchodźców w Polsce

Wsparcie integracyjne i prawne dla uchodźców w Polsce stanowi jeden z kluczowych aspektów działalności organizacji pozarządowych, mający na celu ułatwienie migrantom odnalezienia się w nowym społeczeństwie oraz zapewnienie im odpowiedniej ochrony prawnej. Integracja uchodźców jest procesem wielowymiarowym, który obejmuje naukę języka, edukację, dostęp do rynku pracy, doradztwo administracyjne, a także uczestnictwo w życiu społecznym i kulturalnym. Organizacje pozarządowe pełnią w tym procesie istotną rolę, uzupełniając działania administracji publicznej oraz eliminując bariery, z którymi uchodźcy często się spotykają.

[11] A. Grzymała-Kazłowska, R. Stefańska, *Uchodźcy w Polsce*, BAS, 19(43), 2008, s. 3.

[12] K. Zalas-Kamińska, *Rola organizacji pozarządowych w kampaniach społecznych na rzecz pomocy rozwojowej*, Media, kultura, komunikacja społeczna, 10/3, 2014, s. 32.

Jednym z pierwszych wyzwań, przed jakimi stają uchodźcy w Polsce, jest brak znajomości języka polskiego, co znacznie utrudnia funkcjonowanie w nowym środowisku oraz dostęp do rynku pracy. Dlatego organizacje pozarządowe prowadzą kursy językowe, które pozwalają migrantom na zdobycie podstawowych umiejętności komunikacyjnych. Fundacja Ocalenie czy Polska Akcja Humanitarna oferują bezpłatne zajęcia z języka polskiego na różnych poziomach zaawansowania, dostosowane zarówno do dzieci, jak i dorosłych. Znajomość języka jest kluczowa nie tylko dla codziennego funkcjonowania, ale również dla dalszej edukacji i możliwości podjęcia zatrudnienia.

Równie istotnym aspektem integracji jest dostęp do edukacji dla dzieci uchodźców. Wiele z nich trafia do polskich szkół z opóźnieniami edukacyjnymi, wynikającymi z przerw w nauce spowodowanych wojną lub innymi trudnymi doświadczeniami[13]. Organizacje NGO wspierają ich proces adaptacyjny, organizując zajęcia wyrównawcze, pomoc pedagogiczną oraz wsparcie psychologiczne. Współpracują również ze szkołami, dostarczając materiały dydaktyczne i szkoląc nauczycieli, aby lepiej przygotować ich do pracy z uczniami pochodzącymi z różnych środowisk kulturowych.

Dostęp do rynku pracy to kolejny istotny obszar wsparcia oferowanego przez organizacje pozarządowe. Wielu uchodźców posiada kwalifikacje zawodowe, które nie są uznawane w Polsce, co stanowi poważną barierę w znalezieniu zatrudnienia zgodnego z ich kompetencjami[14]. Organizacje takie jak Fundacja Ocalenie prowadzą programy doradztwa zawodowego, pomagając uchodźcom w zdobyciu kwalifikacji uznawanych na polskim rynku pracy, organizując kursy zawodowe oraz ułatwiając kontakt z potencjalnymi pracodawcami. Programy mentoringowe i praktyki zawodowe oferowane przez NGO pozwalają migrantom zdobyć doświadczenie zawodowe i stopniowo integrować się ze społeczeństwem.

Równolegle do działań integracyjnych niezwykle istotne jest wsparcie prawne i administracyjne. Proces ubiegania się o ochronę międzynarodową w Polsce jest skomplikowany i wymaga odpowiedniego przygotowania formalnego. Wiele organizacji pozarządowych oferuje uchodźcom doradztwo prawne, pomagając im w składaniu wniosków o status uchodźcy, odwołaniach od decyzji administracyjnych oraz w sprawach związanych z legalizacją

[13] M. Pacek, *Proces deinstytucjonalizacji integracji migrantów w Polsce ze szczególnym uwzględnieniem dzieci*, Studia i analizy. Studia Politologiczne, vol. 74, 2024, s. 336.

[14] M. Pawlak, I. Laschuk, *Dostęp do rynku pracy, ale nie do państwa: Sytuacja pracowników migrujących w Polsce*, Friedrich-Ebert-Stiftung 2020, s. 17.

pobytu. Helsińska Fundacja Praw Człowieka oraz Stowarzyszenie Interwencji Prawnej angażują się w ochronę praw migrantów, monitorując sytuację uchodźców i interweniując w przypadkach naruszeń ich podstawowych praw.

Integracja społeczna to kolejny kluczowy aspekt działalności NGO, mający na celu przeciwdziałanie izolacji i marginalizacji uchodźców. Strategia migracyjna zakłada m.in. utworzenie 49 Centrów Integracji Cudzoziemców, w różnych regionach Polski. Nowe centra mają być jednym z instrumentów integracji imigrantów w polskim społeczeństwie[15].

Organizacje pozarządowe organizują również wydarzenia kulturalne, spotkania międzykulturowe, warsztaty i programy społeczne, które pozwalają migrantom nawiązać kontakty z lokalną społecznością. Przykładem takich działań są festiwale wielokulturowe, zajęcia artystyczne czy projekty edukacyjne promujące dialog międzykulturowy. Inicjatywy te nie tylko ułatwiają uchodźcom odnalezienie się w nowym środowisku, ale również budują pozytywne relacje między migrantami a społecznością przyjmującą, przeciwdziałając uprzedzeniom i stereotypom[16].

Działania organizacji pozarządowych w zakresie integracji i wsparcia prawnego uchodźców mają ogromne znaczenie w procesie ich adaptacji do nowego życia w Polsce. Wspierając migrantów na różnych etapach ich pobytu, NGO przyczyniają się do budowania bardziej otwartego i inkluzywnego społeczeństwa. Jednak skuteczność tych działań często zależy od dostępności funduszy, współpracy z administracją publiczną oraz zmieniających się regulacji prawnych. Mimo trudności organizacje pozarządowe odgrywają niezastąpioną rolę w zapewnieniu uchodźcom realnych szans na stabilizację i rozwój w nowym kraju.

Wyzwania i przyszłość działań organizacji pozarządowych w zakresie bezpieczeństwa humanitarnego

Działalność organizacji pozarządowych w zakresie zapewniania bezpieczeństwa humanitarnego uchodźców w Polsce wiąże się z wieloma

[15] *Strategia migracyjna. Powstanie 49 Centrów Integracji Cudzoziemców. Są już szczegóły dotyczące lokalizacji i kosztów CIC,* Infor.pl, https://www.infor.pl/prawo/nowosci-prawne/6737746,strategia-migracyjna-powstanie-49-centrow-integracji-cudzoziemcow-sa.html, [dostęp: 14.03.2025].

[16] E. A. Sowa-Behtane, *Integracja imigrantów ze społeczeństwem przyjmującym. Na przykładzie uczestnictwa w tradycjach, świętach, uroczystościach i życiu kulturalnym*, SPI, Vol. 26, 2023, s. 184.

wyzwaniami, które utrudniają skuteczną pomoc oraz długofalową integrację migrantów. W obliczu narastających kryzysów migracyjnych i zmieniających się uwarunkowań politycznych, organizacje te muszą zmagać się z ograniczeniami finansowymi, barierami biurokratycznymi oraz trudnościami we współpracy z administracją państwową. Pomimo tych przeciwności ich rola w systemie wsparcia humanitarnego pozostaje nieoceniona, a przyszłość ich działań zależy od wielu czynników, w tym polityki migracyjnej Polski oraz możliwości wprowadzenia bardziej efektywnych rozwiązań w zakresie pomocy uchodźcom.

Jednym z największych wyzwań, przed którymi stoją organizacje pozarządowe, jest niestabilność finansowa. NGO w dużej mierze opierają swoją działalność na funduszach pochodzących z dotacji, grantów międzynarodowych oraz darowizn od osób prywatnych i firm. Brak stałego finansowania sprawia, że wiele organizacji ma trudności z planowaniem długoterminowych projektów i zatrudnianiem wykwalifikowanych specjalistów. Szczególnie problematyczne są sytuacje, w których nagłe kryzysy migracyjne, jak w przypadku wojny w Ukrainie, powodują gwałtowny wzrost zapotrzebowania na pomoc humanitarną, a dostępne środki nie są wystarczające, aby sprostać rosnącym potrzebom. Wiele organizacji zmaga się również z ograniczeniami w dostępie do funduszy publicznych, ponieważ część środków rządowych jest rozdzielana w sposób nieprzejrzysty lub warunkowana określonymi kryteriami politycznymi.

Kolejnym istotnym problemem są bariery biurokratyczne, które utrudniają efektywne działanie organizacji pozarządowych. Procesy administracyjne związane z rejestracją organizacji, pozyskiwaniem funduszy oraz uzyskiwaniem pozwoleń na prowadzenie określonych działań, są często skomplikowane i czasochłonne. Dodatkowo zmieniające się przepisy dotyczące migracji i ochrony międzynarodowej sprawiają, że organizacje muszą nieustannie dostosowywać swoje działania do nowych regulacji prawnych, co wymaga dodatkowych zasobów i wysiłku organizacyjnego. Brak jednolitej polityki państwa w zakresie wsparcia NGO oraz różnice w podejściu poszczególnych instytucji publicznych do współpracy z organizacjami społecznymi, dodatkowo utrudniają skuteczne działanie.

Współpraca organizacji pozarządowych z administracją państwową jest kolejnym kluczowym wyzwaniem. Choć w wielu przypadkach NGO współdziałają z władzami lokalnymi oraz instytucjami rządowymi w zakresie pomocy uchodźcom, to relacje te nie zawsze są harmonijne. Niektóre

organizacje napotykają na brak wsparcia ze strony administracji, a nawet na otwartą niechęć ze względu na różnice w podejściu do polityki migracyjnej. W sytuacjach kryzysowych, takich jak nagły napływ uchodźców, współpraca między NGO a państwem jest niezbędna do skutecznego zarządzania pomocą humanitarną, jednak w wielu przypadkach biurokratyczne ograniczenia i brak koordynacji prowadzą do opóźnień oraz niespójności w działaniach.

Rosnąca skala migracji i zmieniająca się sytuacja geopolityczna stawiają przed organizacjami pozarządowymi kolejne wyzwania. Ważnym czynnikiem pożądanych zmian w polskim trzecim sektorze może okazać się wielokrotnie przywoływana tutaj Unia Europejska, która wyznacza wiele norm w dziedzinie krajowych polityk publicznych[17].

W ostatnich latach Polska stała się krajem docelowym dla coraz większej liczby uchodźców, nie tylko z Ukrainy, ale także z Bliskiego Wschodu, Afryki oraz Azji Centralnej. Wzrost liczby osób poszukujących schronienia wymaga zwiększenia zasobów organizacyjnych i finansowych NGO, a także opracowania nowych strategii integracji, które pozwolą uchodźcom szybciej odnaleźć się w polskim społeczeństwie. Ponadto rosnąca polaryzacja społeczna w kwestii migracji oraz przypadki ksenofobii i dyskryminacji utrudniają skuteczną integrację migrantów, co dodatkowo zwiększa rolę organizacji pozarządowych jako podmiotów wspierających dialog społeczny i przeciwdziałających wykluczeniu uchodźców.

Przyszłość działań organizacji pozarządowych w zakresie bezpieczeństwa humanitarnego zależy od kilku kluczowych czynników. Przede wszystkim konieczne jest zapewnienie stabilnego systemu finansowania NGO, który umożliwi im długoterminowe planowanie i rozwój. Wsparcie państwowe oraz większe zaangażowanie sektora prywatnego mogą znacząco zwiększyć skuteczność organizacji humanitarnych[18]. Ważnym elementem jest także uproszczenie procedur administracyjnych i stworzenie bardziej przejrzystego systemu współpracy między organizacjami pozarządowymi a instytucjami państwowymi. Usprawnienie komunikacji i koordynacji działań między różnymi podmiotami zajmującymi się pomocą uchodźcom, mogłoby zwiększyć efektywność wsparcia humanitarnego i skrócić czas reakcji na kryzysy migracyjne.

[17] J. Meisel-Dobrzański, *Współpraca NGO z sektorem publicznym – sposób na wzmocnienie demokracji i wzrost jakości polityk publicznych w Polsce*, Zarządzanie Publiczne, nr 1, 2014, s. 89.

[18] M. Stefańska, *Instytucjonalizacja międzynarodowej współpracy humanitarnej – zagadnienia podstawowe*, Themis Polska Nova, 1(2), 2012, s. 394.

Kolejnym istotnym kierunkiem działań jest rozwój programów integracyjnych, które pozwolą uchodźcom na szybsze wejście na rynek pracy, dostęp do edukacji oraz pełne uczestnictwo w życiu społecznym. Wspieranie inicjatyw kulturalnych i międzykulturowych, przeciwdziałanie dezinformacji na temat migrantów oraz budowanie pozytywnego wizerunku uchodźców w mediach, mogą przyczynić się do większej akceptacji społecznej i zmniejszenia napięć w debacie publicznej. Na poniższym rysunku przedstawiono zjawiska, które w opinii organizacji będą wpływać na działania na rzecz uchodźców w ciągu najbliższych 2 lat, według raportu Stowarzyszenie Klon/Jawor z 2024 r.



Rysunek 2. Zjawiska, które w opinii organizacji będą wpływać na działania na rzecz uchodźców w ciągu najbliższych 2 lat

Źródło: Kondycja organizacji pozarządowych działających na rzecz uchodźców w Polsce, Raport z badań 2024, Stowarzyszenie klon/jawor, s. 11.

Mimo licznych wyzwań organizacje pozarządowe odgrywają niezastąpioną rolę w zapewnianiu bezpieczeństwa humanitarnego uchodźców w Polsce. Ich działalność stanowi kluczowy element systemu wsparcia migracyjnego i integracyjnego, wypełniając luki w działaniach administracji publicznej oraz reagując na dynamicznie zmieniające się potrzeby migrantów. W przyszłości skuteczność tych organizacji będzie zależała od zdolności do adaptacji, współpracy z różnymi sektorami oraz wdrażania innowacyjnych rozwiązań w zakresie pomocy i integracji uchodźców. Wzmocnienie roli NGO i ich większa integracja z polityką migracyjną państwa mogą przyczynić się do stworzenia bardziej efektywnego i humanitarnego systemu wsparcia dla osób poszukujących schronienia w Polsce.

Podsumowanie

Organizacje pozarządowe odgrywają kluczową rolę w zapewnianiu bezpieczeństwa humanitarnego uchodźców w Polsce, wypełniając luki w systemie pomocy publicznej i dostarczając wsparcie zarówno w wymiarze doraźnym, jak i długoterminowym. Ich działania obejmują szeroki zakres inicjatyw – od zapewnienia podstawowych środków do życia, takich jak żywność, odzież i schronienie, po wsparcie psychologiczne, edukacyjne i prawne, które umożliwia uchodźcom lepszą integrację ze społeczeństwem. W obliczu rosnących wyzwań migracyjnych organizacje te stają się nieodzownym elementem systemu wsparcia, przyczyniając się do tworzenia bardziej spójnej i otwartej polityki migracyjnej w Polsce.

Pomimo ich ogromnego zaangażowania organizacje pozarządowe napotykają liczne trudności, które znacząco utrudniają im skuteczne działanie. Główne wyzwania to niestabilność finansowa, skomplikowane procedury administracyjne oraz ograniczona współpraca z administracją publiczną. Wiele NGO boryka się z problemem braku długoterminowego finansowania, co prowadzi do trudności w realizacji większych projektów i ogranicza ich zdolność do szybkiego reagowania na nagłe kryzysy migracyjne. Ponadto złożoność procedur prawnych dotyczących legalizacji pobytu uchodźców oraz zmieniające się regulacje prawne sprawiają, że NGO muszą nieustannie dostosowywać swoje działania do nowych warunków. Brak systematycznej i transparentnej współpracy między państwem a organizacjami społecznymi stanowi dodatkową barierę, która ogranicza możliwości skutecznego wsparcia uchodźców w Polsce.

Pomimo tych trudności organizacje pozarządowe odgrywają niezastąpioną rolę w procesie integracji migrantów. Dzięki ich działaniom uchodźcy mają możliwość nauki języka, zdobycia nowych kwalifikacji zawodowych i znalezienia pracy, co przyczynia się do ich większej samodzielności oraz integracji ze społeczeństwem. Ponadto inicjatywy społeczne i kulturalne organizowane przez NGO sprzyjają budowaniu pozytywnego wizerunku uchodźców, co jest szczególnie istotne w kontekście narastających napięć społecznych i wzrastającej polaryzacji debaty publicznej na temat migracji.

W kontekście narastających napięć społecznych związanych z migracją, ważne jest przeprowadzenie badań nad postawami społecznymi wobec uchodźców oraz ich wpływem na skuteczność działań integracyjnych. Zrozumienie mechanizmów kształtowania opinii publicznej oraz czynników wpływających na akceptację lub odrzucenie migrantów w polskim społeczeństwie

może pomóc w opracowaniu skuteczniejszych strategii komunikacyjnych oraz inicjatyw promujących dialog międzykulturowy.

Literatura

1. Caritas Polska, https://caritas.pl/.
2. Fundacja Ocalenie, https://ocalenie.org.pl/.
3. Grzymała-Kazłowska A., Stefańska R., *Uchodźcy w Polsce*, „BAS", 19(43), 2008.
4. Helsińska Fundacja Praw Człowieka, https://hfhr.pl/.
5. Jasiecki K.*, Pomoc humanitarna dla uchodźców z Ukrainy jako katalizator nowej aktywności społecznej w Polsce*, Studia Politologiczne, nr 68, 2023.
6. Jurek K., *Działalność organizacji pozarządowych w kontekście kryzysu na granicy polsko-białoruskiej (2021-2022)*, Wschodnioznawstwo, nr 16, 2022.
7. *Kondycja organizacji pozarządowych działających na rzecz uchodźców w Polsce*, Raport z badań 2024, Stowarzyszenie klon/jawor.
8. Mianowski J., *Dostęp imigrantek i imigrantów do systemu opieki zdrowotnej w województwie pomorskim – konstruowanie pola międzysektorowej współpracy*, Władza Sądzenia, 16, 2019.
9. Meisel-Dobrzański J., *Współpraca NGO z sektorem publicznym – sposób na wzmocnienie demokracji i wzrost jakości polityk publicznych w Polsce*, Zarządzanie Publiczne, nr 1, 2014.
10. Pacek M., *Proces deinstytucjonalizacji integracji migrantów w Polsce ze szczególnym uwzględnieniem dzieci*, Studia i analizy. Studia Politologiczne, vol. 74, 2024.
11. Pawlak M., Laschuk I., *Dostęp do rynku pracy, ale nie do państwa: Sytuacja pracowników migrujących w Polsce*, Friedrich-Ebert-Stiftung, 2020.
12. Polska Akcja Humanitarna - Międzynarodowa organizacja charytatywna non-profit, https://www.pah.org.pl/.
13. Sowa-Behtane E. A., *Integracja imigrantów ze społeczeństwem przyjmującym. Na przykładzie uczestnictwa w tradycjach, świętach, uroczystościach i życiu kulturalnym*, SPI, Vol. 26, 2023/1.
14. Stefańska M., *Instytucjonalizacja międzynarodowej współpracy humanitarnej – zagadnienia podstawowe*, Themis Polska Nova, 1(2), 2012.
15. Stowarzyszenie Interwencji Prawnej, https://interwencjaprawna.pl/.
16. *Strategia migracyjna. Powstanie 49 Centrów Integracji Cudzoziemców. Są już szczegóły dotyczące lokalizacji i kosztów CIC*, Infor.pl, https://www.infor.pl/prawo/nowosci-prawne/6737746,strategia-migracyjna-powstanie-49-centrow-integracji-cudzoziemcow-sa.html.
17. Zalas-Kamińska K., *Rola organizacji pozarządowych w kampaniach społecznych na rzecz pomocy rozwojowej*, Media, kultura, komunikacja społeczna, 10/3, 2014.
18. Zalewska K., Ochyra-Żurawska K., Ciekanowski Z., *Organizacje pozarządowe w systemie bezpieczeństwa państwa*, Studia Administracji i Bezpieczeństwa, 13(13), 2022.
19. Załącznik do uchwały nr 120 Rady Ministrów z dnia 15 października 2024 r. Odzyskać kontrole. Zapewnić bezpieczeństwo. Kompleksowa i odpowiedzialna strategia migracyjna Polski na lata 2025-2030.

mgr Beata Spinek
Menadżerska Akademia Nauk Stosowanych w Warszawie
ORCID: 0000-0003-2141-8361

mgr Malwina Olbrych
ORCID: 0009-0004-2613-2842

dr Waldemar Perdion
Uczelnia Techniczno-Handlowa w Warszawie
ORCID: 0000-0001-6956-8508

dr Sławomir Żurawski
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0001-9527-3391
https://doi.org/10.29316/9788368103199_15

WPŁYW INFRASTRUKTURY DROGOWEJ NA BEZPIECZEŃSTWO W RUCHU DROGOWYM

THE IMPACT OF ROAD INFRASTRUCTURE ON ROAD SAFETY

Streszczenie

Celem badawczym niniejszego rozdziału jest analiza wpływu infrastruktury drogowej na bezpieczeństwo ruchu drogowego oraz identyfikacja skutecznych rozwiązań mających na celu redukcję liczby wypadków. W pierwszej części przedstawiono definicję infrastruktury drogowej, jej rolę w systemie transportowym oraz statystyki wypadków drogowych wraz z analizą ich głównych przyczyn. Druga część omówiła kluczowe aspekty infrastruktury

Summary

The research objective of this chapter is to analyze the impact of road infrastructure on road safety and to identify effective solutions aimed at reducing the number of accidents. The first part presents the definition of road infrastructure, its role in the transport system and statistics of road accidents along with an analysis of their main causes. The second part discussed key aspects of infrastructure affecting safety, such as road geometry,

wpływające na bezpieczeństwo, takie jak geometria dróg, jakość nawierzchni, organizacja skrzyżowań oraz nowoczesne technologie. W ostatniej części zaprezentowano rekomendacje dotyczące modernizacji infrastruktury, przykłady skutecznych rozwiązań oraz propozycje dalszych badań nad optymalizacją systemu transportowego. Główny problem badawczy sformułowano: Jakie elementy infrastruktury drogowej mają największy wpływ na poprawę bezpieczeństwa ruchu drogowego? Postawiona hipoteza badawcza zakłada, że odpowiednio zaprojektowana i utrzymywana infrastruktura drogowa, obejmująca nowoczesne technologie zarządzania ruchem, poprawę jakości nawierzchni oraz optymalizację skrzyżowań, znacząco zmniejsza ryzyko wypadków oraz ich skutki. W badaniu wykorzystano metody teoretyczne, w tym analizę literatury naukowej, przegląd danych statystycznych dotyczących wypadków drogowych oraz studia przypadków skutecznych rozwiązań infrastrukturalnych w różnych krajach. Główny wniosek z przeprowadzonej analizy wskazuje, że bezpieczeństwo ruchu drogowego można znacząco poprawić poprzez kompleksowe podejście obejmujące modernizację infrastruktury, wdrażanie inteligentnych systemów transportowych oraz optymalizację organizacji ruchu, co prowadzi do zmniejszenia liczby wypadków oraz ich skutków.

Słowa kluczowe: infrastruktura drogowa, bezpieczeństwo ruchu drogowego, zarządzanie ruchem, nowoczesne technologie, wypadki drogowe, środki poprawy bezpieczeństwa

surface quality, organization of intersections and modern technologies. The last part presents recommendations for the modernization of infrastructure, examples of effective solutions and proposals for further research on the optimization of the transport system. The main research problem was formulated: Which elements of road infrastructure have the greatest impact on the improvement of road safety? The research hypothesis assumes that properly designed and maintained road infrastructure, including modern traffic management technologies, improvement of pavement quality and optimization of intersections, significantly reduces the risk of accidents and their consequences. The study used theoretical methods, including analysis of scientific literature, a review of statistical data on road accidents, and case studies of successful infrastructure solutions in different countries. The main conclusion of the analysis is that road safety can be significantly improved through a comprehensive approach that includes upgrading infrastructure, implementing intelligent transport systems and optimising traffic organisation, leading to a reduction in the number of accidents and their consequences.

Keywords: road infrastructure, road safety, traffic management, modern technologies, road accidents, measures to improve safety

Wstęp

Bezpieczeństwo w ruchu drogowym jest jednym z kluczowych wyzwań współczesnego systemu transportowego. Wzrost liczby pojazdów, rozwój miast oraz rosnąca mobilność społeczeństwa sprawiają, że infrastruktura drogowa odgrywa kluczową rolę w minimalizowaniu ryzyka wypadków i poprawie warunków podróży. Statystyki wskazują, że wiele zdarzeń drogowych

wynika nie tylko z błędów ludzkich, ale także z nieodpowiedniego zaprojektowania i utrzymania dróg.

Współczesne badania wykazują, że czynniki takie jak geometria drogi, jakość nawierzchni, organizacja skrzyżowań oraz zastosowanie nowoczesnych technologii mogą znacząco wpływać na poziom bezpieczeństwa użytkowników dróg. Infrastruktura drogowa powinna nie tylko umożliwiać sprawne przemieszczanie się, ale także minimalizować skutki potencjalnych błędów kierowców, pieszych oraz rowerzystów.

Celem niniejszego rozdziału jest analiza wpływu infrastruktury drogowej na bezpieczeństwo ruchu drogowego. Przedstawione zostaną kluczowe aspekty konstrukcji dróg, ich utrzymania oraz nowoczesnych rozwiązań technologicznych, które przyczyniają się do redukcji liczby wypadków. Na podstawie dostępnych badań oraz analiz eksperckich sformułowane zostaną rekomendacje dotyczące projektowania i modernizacji infrastruktury drogowej, w celu zwiększenia bezpieczeństwa wszystkich uczestników ruchu.

Definicja infrastruktury drogowej oraz jej rola w systemie transportowym

Infrastruktura drogowa stanowi kluczowy element systemu transportowego, który obejmuje zarówno fizyczne elementy dróg, jak i ich otoczenie, wpływające na organizację i bezpieczeństwo ruchu. Nowoczesna infrastruktura transportowa stanowi kluczowy element realizacji szybkiego transportu ładunków i osób[1], ale także zapewnia bezpieczeństwo wszystkim uczestnikom ruchu drogowego. Z tego powodu powinna być utrzymywana i rozwijana zgodnie z najwyższymi standardami[2].

Pojęcie „infrastruktura" nie jest jednoznaczne i w literaturze występuje wiele definicji[3]. Na ich podstawie można stworzyć ogólną definicję, która mówi, że infrastruktura drogowa to zbiór obiektów inżynieryjnych, takich jak jezdnie, skrzyżowania, chodniki, oznakowanie poziome i pionowe, sygnalizacja świetlna, a także elementy poprawiające bezpieczeństwo, np. bariery ochronne i oświetlenie uliczne.

[1] M. Kramarz, K. Dohn, E. Przybylska, L. Knop, *Scenarios forthe Development of Multimodal Transport in the TRITIACross-Border Area*, Sustainability, nr 12(17), 2020, s. 3.

[2] M. Urbański, J. Sudyka, K. Grondys, *Ocena ekspercka zarządzania infrastrukturą drogową*, Drogi i mosty, 20, 2021, s. 466.

[3] A. Jasińska, M. Jasiński, *Analiza porównawcza poziomu rozwoju infrastruktury drogowej w Polsce*, Studia Ekonomiczne, nr 1, 2018, s. 146.

Rola infrastruktury drogowej jest wielowymiarowa. Przede wszystkim zapewnia ona efektywne przemieszczanie się osób i towarów, minimalizując czas podróży i koszty operacyjne transportu. Jednocześnie dobrze zaprojektowana i utrzymana infrastruktura wpływa na bezpieczeństwo ruchu drogowego, ograniczając liczbę kolizji oraz zmniejszając ich skutki. W literaturze możemy odnaleźć trzy kategorie korzyści wynikających z budowy czy modernizacji infrastruktury transportu. Są to:

- wymierne wartościowo: koszty eksploatacyjne środków transportu, skrócenie czasu podróży, przesunięcia międzygałęziowe w transporcie, zmiany wartości nieruchomości, wzrost aktywności ekonomicznej;
- społeczno-ekonomiczne: redystrybucja dochodu pomiędzy regionami i grupami społeczno-gospodarczymi, redystrybucja między różnymi użytkownikami, spadek bezrobocia;
- ochrona środowiska i bezpieczeństwa: wpływ na poziom zanieczyszczenia powietrza i hałas, a także bezpieczeństwo[4].

Współczesne rozwiązania inżynieryjne, takie jak inteligentne systemy transportowe (ITS) czy nowoczesne zarządzanie ruchem, odgrywają kluczową rolę w optymalizacji funkcjonowania dróg i redukcji ryzyka wypadków.

Bezpieczeństwo na drogach jest globalnym wyzwaniem, a analiza statystyk wypadków pozwala na identyfikację kluczowych zagrożeń i kierunków działań prewencyjnych. Według danych Światowej Organizacji Zdrowia (WHO), każdego roku na drogach ginie około 1,3 miliona osób, a miliony doznają obrażeń. W Polsce w 2024 roku odnotowano ponad 20 tysięcy wypadków drogowych, w których zginęło około 2 tysięcy osób, a ponad 24 tysiące zostało rannych[5]. Główne przyczyny wypadków drogowych można podzielić na trzy kategorie:

- błędy ludzkie – nadmierna prędkość, nieustąpienie pierwszeństwa, jazda pod wpływem alkoholu, nieprawidłowe manewry[6];
- czynniki infrastrukturalne – złe oznakowanie, niebezpieczne skrzyżowania, brak odpowiedniego oświetlenia, zły stan nawierzchni;

[4] A. Domańska, *Wpływ infrastruktury transportu drogowego na rozwój regionalny*, Wydawnictwo Naukowe PWN, Warszawa 2006, s. 79-80.

[5] Wypadki drogowe. Wstępny bilans 2024 roku - było niebezpiecznie na polskich drogach, Jedź Bezpiecznie, https://jedz-bezpiecznie.pl/wstepny-bilans-2024-roku-bylo-niebezpiecznie-na-polskich-drogach-20250109, [dostęp: 27.02.2025 r.].

[6] E. Brożyna, *Czynnik ludzki a bezpieczeństwo w ruchu drogowym*, Autobusy: technika, eksploatacja, systemy transportowe, R. 18, nr 7-8, 2017, s. 50.

- warunki atmosferyczne i techniczne – opady deszczu, mgła, oblodzenie jezdni, awarie pojazdów.

Badania wskazują, że infrastruktura drogowa odgrywa istotną rolę w ograniczaniu skutków błędów ludzkich oraz eliminacji zagrożeń wynikających z uwarunkowań środowiskowych. Poprawnie zaprojektowane skrzyżowania, dobrze oznakowane drogi oraz odpowiednie systemy zarządzania ruchem mogą znacząco zmniejszyć ryzyko kolizji. Podsumowując, istnieje szeroka gama badań naukowych potwierdzających, że odpowiednio zaprojektowana i utrzymywana infrastruktura drogowa ma kluczowe znaczenie dla bezpieczeństwa ruchu drogowego.

Kluczowe aspekty infrastruktury wpływające na bezpieczeństwo

Bezpieczeństwo ruchu drogowego w dużej mierze zależy od jakości i funkcjonalności infrastruktury drogowej. Odpowiednio zaprojektowane drogi, dobrze utrzymana nawierzchnia, bezpieczne skrzyżowania oraz nowoczesne technologie, mogą znacząco zmniejszyć ryzyko wypadków i poprawić komfort podróżowania. Kluczowe aspekty infrastruktury, takie jak geometria drogi, jakość nawierzchni, organizacja skrzyżowań oraz dodatkowe elementy zabezpieczające, mają istotny wpływ na sposób poruszania się pojazdów i bezpieczeństwo wszystkich uczestników ruchu. Współczesne rozwiązania inżynieryjne oraz inteligentne systemy transportowe pozwalają na skuteczne zarządzanie ruchem i minimalizację zagrożeń.

Geometria drogi odgrywa kluczową rolę w bezpieczeństwie ruchu drogowego, wpływając na sposób poruszania się pojazdów oraz komfort jazdy. Szerokość pasów ruchu ma istotne znaczenie – zbyt wąskie pasy mogą prowadzić do zwiększonego ryzyka kolizji czołowych, natomiast zbyt szerokie mogą skłaniać kierowców do rozwijania nadmiernej prędkości. Optymalne rozwiązania konstrukcyjne uwzględniają także odpowiednie profilowanie zakrętów i łuków, które pozwala na płynne prowadzenie pojazdów i zmniejsza ryzyko utraty kontroli. Dodatkowym czynnikiem poprawiającym bezpieczeństwo jest odpowiednie oznakowanie poziome i pionowe. Czytelne i dobrze utrzymane linie na jezdni, a także jednoznaczne znaki drogowe, umożliwiają kierowcom szybkie podejmowanie decyzji i zapobiegają nieporozumieniom na drodze.

Jakość nawierzchni jest kolejnym istotnym aspektem wpływającym na poziom bezpieczeństwa ruchu drogowego. Drogi w złym stanie technicznym, posiadające liczne nierówności, koleiny czy ubytki, mogą prowadzić do

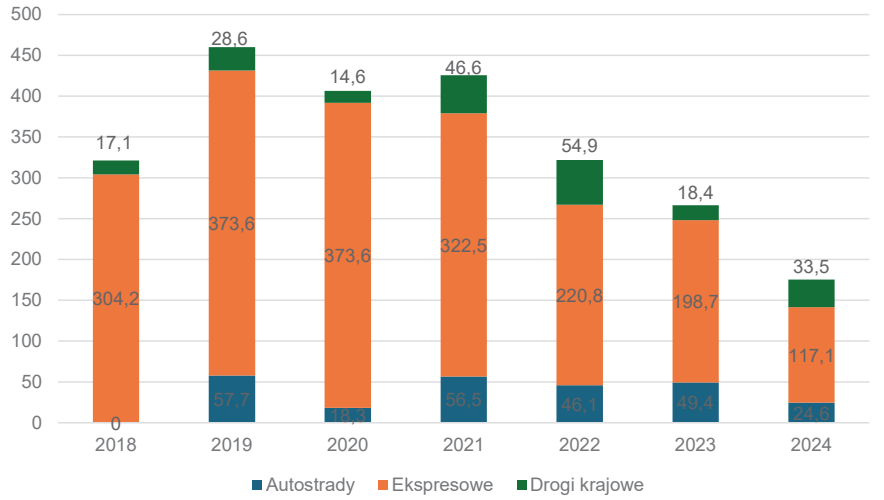
utraty przyczepności, a w konsekwencji do wypadków. Regularne utrzymanie nawierzchni, w tym jej naprawa i stosowanie nowoczesnych materiałów, zmniejsza ryzyko niebezpiecznych sytuacji. Jednym z kluczowych elementów w zapewnieniu bezpieczeństwa jest również efektywne odwodnienie drogi. Zalegająca na jezdni woda może prowadzić do zjawiska aquaplaningu, które powoduje utratę kontroli nad pojazdem. Współczesne technologie pozwalają na budowę dróg z nawierzchnią o właściwościach hydrofobowych, które poprawiają przyczepność i skracają drogę hamowania nawet w trudnych warunkach atmosferycznych. Aby lepiej zobrazować poprawienie się stanu polskich dróg w poniższej tabeli przestawiono długość sieci dróg szybkiego ruchu (A i S) w Polsce w latach 2016-2023.

Tabela 1. Długość sieci dróg szybkiego ruchu (A i S) w Polsce w latach 2016-2023

Rok	Autostrady (km)	Drogi ekspresowe (km)	Razem (km)
2016	1627,3	1533,7	3161,0
2017	1627,3	1808,9	3436,2
2018	1638,5	2092,2	3730,7
2019	1696,2	2450,3	4146,4
2020	1712,0	2557,0	4269,0
2021	1753,6	2871,3	4624,9
2022	1799,7	3087,4	4887,1
2023	1849,4	3266,4	5115,6

Źródło: opracowanie własne na podstawie danych GDDKiA.

Dobry stan infrastruktury drogowej oraz rozwinięta sieć połączeń drogowych wpływają znacznie na natężenie ruchu drogowego oraz przepustowość dróg, co zwiększa poziom bezpieczeństwa. Poniżej przedstawiono zestawienie oddanych dróg w latach 2018-2024.



Rysunek 1. Zestawienie oddanych dróg w latach 2018-2024
Źródło: opracowanie własne na podstawie danych GDDKiA.

Skrzyżowania należą do najbardziej newralgicznych punktów w infrastrukturze drogowej, ponieważ to właśnie w tych miejscach dochodzi do największej liczby kolizji i wypadków[7]. Poniżej w tabeli przedstawiono wybrane miejsca ruchu pieszych.

Tabela 2. Wybrane miejsca ruchu pieszych

Wybrane miejsca ruchu pieszych	Wypadki	Zabici	Ranni
Przejścia dla pieszych	2 684	132	2 658
Skrzyżowanie	1 055	61	1 022
Chodnik droga dla pieszych	327	17	314
Pobocze	40	9	40
Przystanek komunikacji publicznej	45	3	43

Źródło: Wypadki drogowe w Polsce, Komenda Główna Policji, Biuro Ruchu Drogowego, Warszawa 2024.

Jak wynika z powyższych danych to skrzyżowania są jednym z najczęstszych miejsc wypadków. Sygnalizacja świetlna, jeśli jest odpowiednio zaprogramowana i dostosowana do natężenia ruchu, może znacząco poprawić płynność ruchu i zmniejszyć liczbę niebezpiecznych zdarzeń. Wprowadzenie

[7] R. Kozłowski, *Zależności między infrastrukturą transportu a poziomem bezpieczeństwa ruchu drogowego na drogach krajowych województwa łódzkiego*, Seria SWSPiZ: Przedsiębiorczość i Zarządzanie, Tom XII, Zeszyt 9, 2011, s. 194.

rond w miejsce klasycznych skrzyżowań również przyczynia się do poprawy bezpieczeństwa. Badania wykazują, że liczba wypadków na skrzyżowaniach o ruchu okrężnym jest znacznie mniejsza w porównaniu do skrzyżowań ze światłami, głównie ze względu na zmniejszoną prędkość pojazdów i ograniczenie liczby punktów kolizyjnych. Coraz większe znaczenie mają również inteligentne systemy transportowe, które wykorzystują technologie monitorowania ruchu w czasie rzeczywistym, pozwalając na dynamiczne zarządzanie sygnalizacją świetlną i kierowaniem strumieni pojazdów.

Bezpieczeństwo na drogach w dużej mierze zależy także od dodatkowych elementów infrastruktury, które mają za zadanie chronić uczestników ruchu i minimalizować skutki ewentualnych wypadków. Bariery ochronne skutecznie zapobiegają wypadnięciu pojazdów z drogi, a także ograniczają skutki kolizji czołowych. Oświetlenie uliczne jest kluczowe, szczególnie w obszarach o dużym natężeniu ruchu pieszego, ponieważ poprawia widoczność zarówno kierowców, jak i pieszych. Dobrze zaprojektowane przejścia dla pieszych, wyposażone w sygnalizację świetlną lub dodatkowe podwyższenia, zwiększają bezpieczeństwo niechronionych uczestników ruchu. Separacja ruchu pieszego i rowerowego od ruchu samochodowego, pozwala na ograniczenie liczby kolizji i poprawia komfort wszystkich uczestników ruchu drogowego.

Nowoczesne technologie w infrastrukturze drogowej odgrywają coraz większą rolę w poprawie bezpieczeństwa. Inteligentne systemy zarządzania ruchem umożliwiają monitorowanie natężenia ruchu i optymalizację pracy sygnalizacji świetlnej, co zmniejsza ryzyko wypadków spowodowanych zatorami drogowymi. Rozwój pojazdów autonomicznych oraz ich integracja z infrastrukturą drogową stanowi kolejny krok w kierunku bezpieczniejszego transportu. Inteligentne drogi, wyposażone w systemy komunikacji z pojazdami, mogą ostrzegać kierowców o niebezpiecznych warunkach czy zbliżających się przeszkodach, co pozwala na szybszą reakcję i uniknięcie kolizji. Nowoczesne systemy monitorowania, wykorzystujące kamery i czujniki, umożliwiają wykrywanie niebezpiecznych sytuacji na drodze i szybką interwencję odpowiednich służb.

W literaturze naukowej oraz raportach zarówno instytucji krajowych i międzynarodowych, istnieje wiele badań dotyczących wpływu infrastruktury drogowej na bezpieczeństwo ruchu drogowego. Wśród najważniejszych ustaleń warto wymienić:

- geometria drogi i bezpieczeństwo – badania prowadzone przez European Road Safety Observatory (ERSO) wykazały, że nieprawidłowa geometria dróg, w tym zbyt ostre łuki poziome i pionowe oraz zbyt wąskie pasy ruchu, zwiększa ryzyko wypadków[8].
- efektywność rond w redukcji wypadków – analiza przeprowadzona przez National Highway Traffic Safety Administration (NHTSA) wykazała, że wprowadzenie rond zamiast tradycyjnych skrzyżowań zmniejsza liczbę poważnych kolizji nawet o 40%, głównie dzięki redukcji punktów kolizyjnych i wymuszeniu zmniejszenia prędkości[9].
- wpływ oznakowania i sygnalizacji świetlnej – badania dowodzą, że czytelne oznakowanie poziome oraz odpowiednio zaprogramowana sygnalizacja świetlna znacznie poprawiają bezpieczeństwo na drogach o dużym natężeniu ruchu. W szczególności stwierdzono, że systemy adaptacyjne dostosowujące długość sygnałów świetlnych do natężenia ruchu, mogą redukować ryzyko kolizji na skrzyżowaniach o nawet 30%.
- jakość nawierzchni i jej wpływ na wypadkowość – prace naukowe wskazują, że niski współczynnik przyczepności nawierzchni (np. z powodu nierówności, kolein czy złej jakości asfaltu), może prowadzić do zwiększonego ryzyka poślizgów i wydłużenia drogi hamowania. Regularna konserwacja nawierzchni i stosowanie nowoczesnych materiałów (np. asfaltu o wysokiej odporności na deformacje), mogą ograniczyć liczbę wypadków związanych z utratą kontroli nad pojazdem.

Infrastruktura drogowa ma ogromny wpływ na poziom bezpieczeństwa w ruchu drogowym. Odpowiednio zaprojektowane drogi, dobrej jakości nawierzchnia, bezpieczne skrzyżowania oraz nowoczesne technologie mogą przyczynić się do znacznej redukcji liczby wypadków. Inwestowanie w rozwój infrastruktury oraz wdrażanie inteligentnych rozwiązań to kluczowe działania na rzecz poprawy bezpieczeństwa uczestników ruchu drogowego.

[8] European Road Safety Observatory - European Commission, https://roadsafety.transport.ec.europa.eu/european-road-safety-observatory_en, [dostęp: 27.02.2025 r.].

[9] *National Highway Traffic Safety Administration (NHTSA)*, National Highway Traffic Safety Administration (NHTSA), [dostęp: 27.02.2025 r.].

Rekomendacje i propozycje dalszych działań nad optymalizacją infrastruktury drogowej w celu zwiększenia bezpieczeństwa w ruchu drogowym

Analiza wpływu infrastruktury drogowej na bezpieczeństwo ruchu drogowego jednoznacznie wskazuje, że odpowiednie projektowanie, modernizacja oraz utrzymanie dróg, mogą znacząco zmniejszyć liczbę wypadków i ich skutków. Kluczowe aspekty, takie jak geometria drogi, jakość nawierzchni, organizacja skrzyżowań, a także separacja ruchu pieszego i rowerowego, odgrywają istotną rolę w zapewnieniu bezpiecznych warunków dla wszystkich uczestników ruchu drogowego.

Nieodpowiednia geometria dróg, w tym zbyt ostre łuki, nieprzystosowana szerokość pasów ruchu oraz brak odpowiednich oznakowań, prowadzi do wzrostu liczby kolizji i groźnych zdarzeń drogowych. Badania wskazują, że wprowadzenie odpowiednich standardów w zakresie projektowania dróg, takich jak minimalizacja ostrych zakrętów, dostosowanie szerokości pasów do charakterystyki ruchu oraz poprawa widoczności poprzez odpowiednie oznakowanie, może znacznie poprawić bezpieczeństwo[10].

Stan nawierzchni dróg ma równie istotne znaczenie. Nierówności, koleiny, ubytki w nawierzchni oraz niewłaściwe odwodnienie mogą przyczyniać się do utraty kontroli nad pojazdem, szczególnie podczas trudnych warunków pogodowych. Stosowanie nowoczesnych materiałów, takich jak mieszanki asfaltowe o podwyższonej odporności na ścieranie oraz specjalistyczne technologie zwiększające przyczepność, pozwala na znaczące zmniejszenie ryzyka poślizgów i wydłużonej drogi hamowania.

Skrzyżowania stanowią jeden z najbardziej niebezpiecznych elementów infrastruktury drogowej, dlatego ich odpowiednia organizacja i projektowanie mają kluczowe znaczenie dla bezpieczeństwa. Wprowadzenie inteligentnych systemów sterowania ruchem, optymalizacja sygnalizacji świetlnej oraz zastępowanie klasycznych skrzyżowań rondami pozwala na znaczną redukcję liczby wypadków, zmniejszenie punktów kolizyjnych oraz poprawę płynności ruchu[11].

[10] J. Barcik, P. Cech, *Wpływ infrastruktury drogowej na bezpieczeństwo ruchu – część 1*, Zeszyty Naukowe Politechniki Śląskiej. Seria: Transport, z. 67, 2010, s. 17.

[11] M. Szruba, *Wybrane czynniki wpływające na bezpieczeństwo w ruchu drogowym*, Nowoczesne Budownictwo Inżynieryjne, Marzec – Kwiecień 2019, s. 3

Nie można również pomijać roli dodatkowych elementów infrastrukturalnych, które zwiększają bezpieczeństwo. Bariery ochronne, oświetlenie uliczne, przejścia dla pieszych wyposażone w aktywne oznakowanie oraz separacja ruchu pieszego i rowerowego od ruchu pojazdów to rozwiązania, które przyczyniają się do znaczącego zmniejszenia liczby kolizji, szczególnie tych z udziałem niechronionych uczestników ruchu[12].

W wielu krajach wdrożono rozwiązania infrastrukturalne, które przyczyniły się do poprawy bezpieczeństwa ruchu drogowego. Jednym z najbardziej efektywnych działań jest wprowadzenie rond zamiast tradycyjnych skrzyżowań z sygnalizacją świetlną. Badania wykazują, że tego typu rozwiązanie zmniejsza liczbę wypadków o około 40%, a liczbę wypadków śmiertelnych nawet o 70%. Wynika to przede wszystkim z ograniczenia liczby punktów kolizyjnych oraz konieczności zmniejszenia prędkości przez kierowców. Innym przykładem skutecznej modernizacji infrastruktury są inteligentne systemy zarządzania ruchem. Systemy te, wykorzystując czujniki i analizę natężenia ruchu, dynamicznie dostosowują sygnalizację świetlną do aktualnej sytuacji na drodze, co pozwala na ograniczenie liczby nagłych zatrzymań, a tym samym zmniejszenie ryzyka kolizji.

W krajach skandynawskich dużą rolę w poprawie bezpieczeństwa odgrywają zaawansowane rozwiązania w zakresie infrastruktury rowerowej i ruchu pieszego. Separacja ruchu rowerowego od ruchu samochodowego poprzez wydzielone ścieżki rowerowe oraz zastosowanie specjalnych barier ochronnych wzdłuż tras rowerowych, pozwala na znaczną redukcję liczby wypadków z udziałem rowerzystów. Dodatkowo stosowanie aktywnych przejść dla pieszych, które wykorzystują czujniki ruchu i sygnalizację świetlną ostrzegającą kierowców o obecności pieszego, skutecznie zmniejsza liczbę potrąceń[13].

Kolejnym wartym uwagi rozwiązaniem jest poprawa jakości nawierzchni poprzez zastosowanie specjalnych mieszanek asfaltowych, które zmniejszają hałas i poprawiają przyczepność. W krajach o częstych opadach atmosferycznych stosuje się porowate nawierzchnie, które skutecznie odprowadzają wodę i zapobiegają powstawaniu kałuż oraz zjawiska aquaplaningu.

[12] A. Wojtas, M. Szkoda, *Analiza wybranych czynników wpływających na bezpieczeństwo w ruchu drogowym*, Autobusy – Technika, Eksploatacja, Systemy Transportowe, vol. 220, nr 6, 2018, s. 1150.

[13] Kompleksowe badanie porównawcze w obszarze bezpieczeństwa ruchu drogowego Norwegii i Polski, Zespół Doradców Gospodarczych, Warszawa 2024, s. 120.

Mimo postępu technologicznego i wdrażania nowych rozwiązań w zakresie infrastruktury drogowej, konieczne jest dalsze prowadzenie badań nad skutecznością różnych metod poprawy bezpieczeństwa. W szczególności warto skupić się na analizie wpływu inteligentnych systemów transportowych oraz automatycznych systemów zarządzania ruchem na redukcję liczby wypadków. Przyszłe badania powinny także koncentrować się na integracji infrastruktury drogowej z pojazdami autonomicznymi. W miarę postępu technologii i rozwoju transportu autonomicznego kluczowe będzie opracowanie systemów komunikacji między pojazdami a infrastrukturą drogową (V2I – Vehicle-to-Infrastructure), które umożliwią szybką wymianę informacji o warunkach drogowych, przeszkodach oraz możliwych zagrożeniach[14].
Ważnym kierunkiem badań jest również analiza wpływu zmian klimatycznych na bezpieczeństwo ruchu drogowego oraz opracowanie nowych materiałów i technologii budowlanych, które będą bardziej odporne na ekstremalne warunki atmosferyczne. Wprowadzenie inteligentnych nawierzchni, które mogą dynamicznie dostosowywać swoje właściwości do panujących warunków (np. poprzez zmianę struktury w zależności od temperatury), może przyczynić się do znaczącego zwiększenia bezpieczeństwa na drogach.

Podsumowując, dalszy rozwój infrastruktury drogowej powinien koncentrować się na wdrażaniu nowoczesnych technologii, optymalizacji organizacji ruchu oraz poprawie jakości dróg i oznakowania. Kluczowe jest również prowadzenie badań nad skutecznością różnych rozwiązań oraz ich dostosowanie do specyficznych warunków geograficznych i klimatycznych. Współpraca między inżynierami, urbanistami i specjalistami ds. bezpieczeństwa ruchu drogowego jest niezbędna, aby tworzyć coraz bardziej efektywne i bezpieczne systemy transportowe.

Podsumowanie

Bezpieczeństwo ruchu drogowego jest jednym z kluczowych wyzwań współczesnego systemu transportowego, a infrastruktura drogowa odgrywa w nim fundamentalną rolę. Analiza wpływu infrastruktury na poziom bezpieczeństwa wykazała, że odpowiednie projektowanie dróg, dbałość o jakość

[14] *What is Vehicle-to-Infrastructure (V2I) Communication and why do we need it?*, https://www.3mindia.in/3M/en_IN/road-safety-in/resources/road-transportation-safety-center-blog/full-story/~/what-is-vehicle-to-infrastructure-v2i-communication-and-why-do-we-need-it/?story-id=0b95359f-9389-4233-9db4-63e307d36b70, [dostęp: 27.02.2025 r.].

nawierzchni, nowoczesne zarządzanie ruchem oraz zastosowanie inteligentnych technologii, mogą znacząco zmniejszyć liczbę wypadków i poprawić komfort podróży.

Jednym z najważniejszych wniosków wynikających z analizy jest fakt, że błędy ludzkie, które są główną przyczyną wypadków, mogą być skutecznie minimalizowane poprzez odpowiednie rozwiązania infrastrukturalne. Odpowiednio zaprojektowane drogi, z czytelnym oznakowaniem i właściwą organizacją ruchu, mogą zmniejszyć ryzyko błędnych decyzji kierowców oraz ich konsekwencji. Kluczowym elementem poprawy bezpieczeństwa jest również modernizacja skrzyżowań, w tym zastępowanie tradycyjnych skrzyżowań rondami oraz wdrażanie inteligentnych systemów zarządzania ruchem, które dostosowują się do aktualnej sytuacji na drodze.

Kolejnym istotnym wnioskiem jest znaczenie jakości nawierzchni. Utrzymanie dróg w dobrym stanie technicznym, stosowanie nowoczesnych materiałów o wysokiej przyczepności oraz efektywne systemy odwodnienia pozwalają na ograniczenie liczby wypadków związanych z trudnymi warunkami atmosferycznymi. W szczególności w rejonach o częstych opadach deszczu lub śniegu odpowiednie technologie nawierzchniowe mogą istotnie poprawić bezpieczeństwo.

Nowoczesne technologie odgrywają coraz większą rolę w poprawie bezpieczeństwa ruchu drogowego. Inteligentne systemy transportowe, adaptacyjne sygnalizacje świetlne, zaawansowane oznakowania oraz integracja infrastruktury drogowej z pojazdami autonomicznymi to przyszłościowe rozwiązania, które mogą znacząco ograniczyć liczbę wypadków. Rozwój technologii komunikacji między pojazdami a infrastrukturą (V2I) oraz wdrażanie systemów predykcyjnych opartych na analizie danych mogą pomóc w przewidywaniu potencjalnych zagrożeń i ich eliminacji, zanim dojdzie do niebezpiecznej sytuacji.

Jednocześnie, mimo dynamicznego rozwoju infrastruktury drogowej, istnieje potrzeba dalszych badań nad optymalizacją systemu transportowego w kontekście bezpieczeństwa. Kluczowym kierunkiem zmian powinny być badania nad efektywnością różnych rozwiązań infrastrukturalnych w rzeczywistych warunkach ruchu oraz nad ich dostosowaniem do lokalnych uwarunkowań geograficznych, demograficznych i klimatycznych. Niezbędne jest również przeprowadzenie szczegółowych analiz dotyczących wpływu autonomicznych pojazdów na organizację ruchu oraz ich integracji z istniejącą infrastrukturą drogową. W perspektywie długoterminowej kluczowym wyzwaniem

będzie również dostosowanie infrastruktury drogowej do rosnących wymagań związanych z ochroną środowiska i zrównoważonym transportem. Rozwój miast wymaga inwestowania w infrastrukturę przyjazną dla pieszych i rowerzystów, a także wdrażania inteligentnych systemów ograniczających emisję spalin i redukujących natężenie ruchu.

Poprawa bezpieczeństwa w ruchu drogowym wymaga kompleksowego podejścia, łączącego modernizację infrastruktury z wykorzystaniem nowoczesnych technologii oraz dalszymi badaniami nad optymalizacją systemu transportowego. Dalsze inwestycje w inteligentne rozwiązania drogowe, badania nad skutecznością poszczególnych metod oraz integracja infrastruktury z systemami wspomagania kierowców i pojazdami autonomicznymi to kluczowe kierunki zmian, które mogą przyczynić się do znaczącej redukcji liczby wypadków i poprawy bezpieczeństwa na drogach.

Literatura

1. Barcik J., Cech P., *Wpływ infrastruktury drogowej na bezpieczeństwo ruchu – część 1*, Zeszyty Naukowe Politechniki Śląskiej. Seria: Transport, z. 67, 2010.
2. Brożyna E., *Czynnik ludzki a bezpieczeństwo w ruchu drogowym*, „Autobusy: technika, eksploatacja, systemy transportowe", R. 18, nr 7-8, 2017.
3. Domańska A., *Wpływ infrastruktury transportu drogowego na rozwój regionalny*, Wydawnictwo Naukowe PWN, Warszawa 2006.
4. European Road Safety Observatory - European Commission, https://roadsafety.transport.ec.europa.eu/european-road-safety-observatory_en.
5. Jasińska A., Jasiński M., *Analiza porównawcza poziomu rozwoju infrastruktury drogowej w Polsce*, Studia Ekonomiczne, nr 1, 2018.
6. Kompleksowe badanie porównawcze w obszarze bezpieczeństwa ruchu drogowego Norwegii i Polski, Zespół Doradców Gospodarczych, Warszawa 2024.
7. Kozłowski R., *Zależności między infrastrukturą transportu a poziomem bezpieczeństwa ruchu drogowego na drogach krajowych województwa łódzkiego*, Seria SWSPiZ: Przedsiębiorczość i Zarządzanie, Tom XII, Zeszyt 9, 2011.
8. Kramarz M., Dohn K., Przybylska E., Knop L., *Scenarios forthe Development of Multimodal Transport in the TRITIACross-Border Area*, Sustainability, nr 12(17), 2020.
9. National Highway Traffic Safety Administration (NHTSA), National Highway Traffic Safety Administration (NHTSA).
10. Szruba M., *Wybrane czynniki wpływające na bezpieczeństwo w ruchu drogowym*, Nowoczesne Budownictwo Inżynieryjne, Marzec – Kwiecień 2019.
11. Urbański M., Sudyka J., Grondys K., *Ocena ekspercka zarządzania infrastrukturą drogową*, Drogi i mosty, 20, 2021.
12. What is Vehicle-to-Infrastructure (V2I) Communication and why do we need it?, https://www.3mindia.in/3M/en_IN/road-safety-in/resources/road-transportation-

safety-center-blog/full-story/~/what-is-vehicle-to-infrastructure-v2i-communication-and-why-do-we-need-it/?storyid=0b95359f-9389-4233-9db4-63e307d36b70.
13. Wypadki drogowe. Wstępny bilans 2024 roku - było niebezpiecznie na polskich drogach, Jedź Bezpiecznie. https://jedz-bezpiecznie.pl/wstepny-bilans-2024-roku-bylo-niebezpiecznie-na-polskich-drogach-20250109.
14. *Wypadki drogowe w Polsce*, Komenda Główna Policji, Biuro Ruchu Drogowego, Warszawa 2024.
15. Wojtas A., Szkoda M., *Analiza wybranych czynników wpływających na bezpieczeństwo w ruchu drogowym*, Autobusy – Technika, Eksploatacja, Systemy Transportowe, vol. 220, nr 6, 2018.

dr Zbigniew Piskor
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID 0000-0002-4456-1104
https://doi.org/10.29316/9788368103199_16

ZARZĄDZANIE ZASOBAMI ZAŁOGI LOTNICZEJ

FLIGHT CREW RESOURCE MANAGEMENT

Streszczenie

Celem rozdziału jest analiza wpływu czynnika ludzkiego i zarządzania zasobami załogi na poziom bezpieczeństwa operacji lotniczych oraz wskazanie skutecznych działań prewencyjnych w celu poprawy bezpieczeństwa w branży lotniczej. Główny problem badawczy sformułowano: Jak zagrożenia wynikające z czynnika ludzkiego wpływają na poziom bezpieczeństwa lotniczego? We wstępie przedstawiono dynamiczny rozwój sektora lotniczego oraz rosnące wyzwania związane z bezpieczeństwem w kontekście globalizacji i wzrostu ruchu lotniczego. W kolejnej części opisano znaczenie komunikacji, współpracy i skutecznego przywództwa w zespole lotniczym oraz rolę szkoleń CRM w minimalizowaniu ryzyka błędów. Następnie wskazano na wysokie wymagania certyfikacyjne oraz koszt i czasochłonność przygotowania do pracy w lotnictwie. Kolejno ukazano rosnące znaczenie kobiet w zawodach lotniczych i ich przełamywanie tradycyjnych barier, podkreślono również znaczenie zarządzania zagrożeniami i błędami

Summary

The aim of the chapter is to analyze the impact of the human factor and crew resource management on the level of safety of air operations and to indicate effective preventive measures to improve safety in the aviation industry. The main research problem was formulated: How do the risks resulting from the human factor affect the level of aviation safety? The introduction presents the dynamic development of the aviation sector and the growing challenges related to safety in the context of globalization and the growth of air traffic. The next part describes the importance of communication, collaboration, and effective leadership in the aviation team, and the role of CRM training in minimizing the risk of errors. Then, the high certification requirements as well as the cost and time of preparation for work in aviation were indicated. The growing importance of women in aviation professions and their overcoming of traditional barriers was also shown, the importance of hazard and error management (TEM), the need to develop situational awareness and continuous improvement of

(TEM), konieczność rozwijania świadomości sytuacyjnej oraz ciągłego doskonalenia procedur bezpieczeństwa. W podsumowaniu wskazano, że dalszy rozwój lotnictwa musi opierać się na inwestycjach w nowe technologie, szkolenia oraz budowanie silnej kultury organizacyjnej opartej na zaufaniu i odpowiedzialności. W rozdziale zastosowano teoretyczne metody badawcze takie jak, krytyczna analiza aktów prawnych, analiza literatury przedmiotu oraz analiza danych branżowych.

Słowa kluczowe: zarządzanie, czynnik ludzki, lotnictwo, bezpieczeństwo, statek powietrzny

safety procedures was also emphasized. In conclusion, it was pointed out that further development of aviation must be based on investments in new technologies, training and building a strong organizational culture based on trust and responsibility. The chapter uses theoretical research methods such as critical analysis of legal acts, analysis of the literature on the subject and analysis of industry data.

Keywords: management, human factor, aviation, security, aircraft

Wstęp

Globalny rozwój transportu lotniczego determinowany jest przemianami i trendami w rozwoju światowej gospodarki przy przewidywanym wzroście ruchu o 4,3% rocznie do roku 2035. Lotniska bez stanowisk check-in? Statki powietrzne bez pilotów, zdalne wieże zarządzania ruchem lotniczym na lotniskach? W przyszłości czekają nas orbitalne loty pasażerskie, czy loty statkami autonomicznymi. Dziś kupno biletu załatwiamy kliknięciem w smartfonie. Jedynie dobra organizacja jest w stanie dać dobre produkty, usługi, stwarza się konieczność wypracowania i stosowania działań globalnych w budowaniu strategii i bezpieczeństwa personalnego w sektorze branży lotniczej.

Liczba wszystkich lotów na całym świecie w 2024 roku wyniosła około 100 mln, co oznacza wzrost o 4,3 proc. do roku 2035. ACI[1] jest organizacją obejmującą 2181 lotnisk w 170 krajach i według analiz przeprowadzonych wskazuje, że pierwsza dziesiątka największych lotnisk odpowiada za 9 procent globalnego ruchu lotniczego, gdzie prym wiodą lotniska USA, jak: Hartsfield-Jackson w Atlancie, Chicago-O'Hare i Dallas. Fort Worth[2]. W Europie mamy Londyńskie Heathrow. Pod względem największego ruchu towarowego znajdują się lotniska w Hongkongu, Szanghaju oraz Memphis w amerykańskim stanie Tennessee, szacuje się, że wolumen ładunków przewożonych drogą

[1] ACI - Airports Council International, Międzynarodowe Zrzeszenie Portów Lotniczych.

[2] *Największy ruch pasażerski w 2024 r. na lotniskach w Atlancie, Dubaju i Dallas*, dlapilota.pl, [dostęp: 20.04.2025].

lotniczą wzrósł o 8,4 procent do 124 mln ton. Lotnisko Szanghaj Pudong, awansowało z 21 pozycji w 2023 r. na dziesiątą pozycję w rankingu 2024 roku. Przewidywany wzrost w globalnym ruchu pasażerskim w 2030 roku przekroczy 12 mld pasażerów, natomiast w 2042 roku ma osiągnąć 19,5 mld., co oznacza dwukrotny wzrost do obecnego roku, a spowodowane jest rozwojem międzynarodowych rynków w regionie Azji i Pacyfiku oraz Bliskiego Wschodu. Z danych Urzędu Lotnictwa Cywilnego lotniska w Polsce w 2024 roku obsłużyły 59,2 mln pasażerów, to o 13,3 proc. więcej niż w 2023 r. i o 20,8 proc. więcej niż w 2019 roku, za wzrost odpowiadają głównie tanie linie lotnicze.

Wzrost przewozu towarów drogą lotniczą wiąże się z dużym popytem w handlu online zapoczątkowanym w czasie sprzed pandemii Covid-19, zakłóceniami w transporcie morskim i spadkiem cen paliwa lotniczego[3]. Już w latach 70-tych ubiegłego wieku dostrzeżono duży negatywny „wkład" w powstawanie incydentów lotniczych poprzez brak efektywnej współpracy personelu lotniczego, czy mówiąc ogólniej, „zła atmosfera" panująca na lotniskach. Zwrócono uwagę na fakt, iż pracownicy nie chcą podważać autorytetu przełożonego. Nawet, jeśli popełnia tragiczny w skutkach błąd, jego współpracownik często milczy, bojąc się konsekwencji, gdyż nie chce „narazić się". Może to przyjąć postać myślenia typu „Jestem młody i niedoświadczony, a przełożony ma duży staż pracy, więc na pewno wie lepiej".

Kluczowe aspekty zarządzania zasobami załogi lotniczej

Lotnictwo jest jedną z tych dziedzin działalności człowieka, które stawiają szczególnie wysokie wymagania przed osobami zaangażowanymi w proces przygotowania i realizacji zadań. Zarządzanie zasobami załogi lotniczej to kluczowy element bezpieczeństwa lotów. Rozwój IT spowodował również rozwój lotnictwa w szerokim tego słowa znaczeniu. Dlatego już dzisiaj musimy widzieć zmieniające się nasze lotnictwo w globalnym świecie. Zapotrzebowanie na pracowników – specjalistów wzrośnie zatem w ciągu najbliższych 20 lat na całym świecie do 770 tys. techników - inżynierów, 800 tys. pilotów, 915 tys. członków personelu pokładowego. Budowane są nowe zakłady pod nowe samoloty, silniki lotnicze, hangary do przeglądów okresowych. Edukacja pracowników, a następnie specjalistów to wyzwanie szkolnictwa na wszystkich poziomach, od szkoły średniej po wyższe uczelnie.

[3] Annual Safety Review 2023, EASA, s. 4.

Chcąc kształcić przyszłe kadry, Ośrodki Szkoleniowe muszą mieć odpowiednie Certyfikaty bądź Decyzję Władzy Lotniczej. Muszą wykazać się zapleczem w postaci kadry dydaktycznej, kadry instruktorskiej oraz zapleczem „warsztatowym" samolotowym, symulatorowym. Za tym muszą być wyłożone środki finansowe na stworzenie, utrzymanie i rozwój bazy. Skupia się na poprawie efektywności komunikacji, przywództwa oraz współpracy w zespole, co przekłada się na lepsze wyniki operacyjne i zwiększoną ochronę pasażerów oraz załogi. Wdrożenie skutecznych praktyk CRM[4] w organizacji lotniczej, ma na celu nie tylko minimalizację ryzyka, ale również budowanie pozytywnej kultury organizacyjnej[5].

Szkolenia CRM zostały zapoczątkowane w liniach US United Airlines w 1981 r. Za tym programem szkoleniowym podążyły inne linie lotnicze[6]. Skupiały się one na problemach zarządzania oraz przejściu od indywidualnych stylów zarządzania do współpracy w załodze[7]. Linie lotnicze zgłaszały, iż największym problemem był niski poziom asertywności pierwszych oficerów i autorytaryzm doświadczonych kapitanów. Obserwowano zjawisko tzw. „kapitanozy". Pierwsze szkolenia kładły nacisk na aspekt psychologiczny przywództwa. Ogromną uwagę skupiano na takim zaprojektowaniu systemu szkoleniowego, by piloci brali udział w treningu corocznie, nie zaś jednorazowo. Program ten był realizowany nie tylko w sali treningowej, ale także łączono go z sesją w symulatorze. Pierwsze treningi oparte na zaktualizowanym programie wprowadziła Delta Airlines. Większy nacisk kładziono na pracę zespołową, a główne elementy, na których oparto program, to:

- budowanie zespołu,
- strategie briefingowe,
- świadomość sytuacyjna,
- zarządzanie stresem,
- odejmowanie decyzji w załodze,
- łańcuch błędów.

[4] CRM – Crew Resource Menagement, Zarządzanie zasobami załogi.

[5] W. Liszkowska, *Zarządzanie zasobami załogi, czyli jak uniknąć błędów zarządczych*, Zeszyty Naukowe. Organizacja i Zarządzanie, 71(1222), 2018, s. 71.

[6] R. Gałązkowski, M. Tomaszewski, *Bezpieczeństwo lotów a szkolenie w zakresie zarządzania zasobami załogi w zarobkowym przewozie lotniczym*, Zeszyty Naukowe AON, nr 2(99), 2015, s, 130.

[7] H. W. Orlandy, H.C. Foushee, *Cockpit Resource Management Training*, Technical Report Number NASA CP-2455, Moffett Field: NASA-Ames Research Center 1987.

Od połowy lat 90. program CRM stał się obowiązkowym modułem w szkoleniu w liniach lotniczych[8]. Naukowcy współpracujący z NASA prowadzili badania nad wyodrębnieniem plusów i minusów prowadzonych szkoleń, a także odpowiedzią na pytanie: czy spełniają one swoją rolę i zwiększają bezpieczeństwo oraz wydajność lotów?

Do największych słabości programu zaliczono fakt, iż nie dociera on do wszystkich, a akceptacja jego podstawowych założeń bardzo rozciąga się w czasie. Zarzucono również, że CRM uczy, jak pracować w zespole. Zamiast, dlaczego praca zespołowa jest tak ważna. Problemem było też dopasowanie szkoleń CRM do specyfikacji konkretnego kraju lub rejonu.

Systemy zarządzania HR w lotnictwie odgrywają kluczową rolę w zapewnieniu efektywnego funkcjonowania organizacji charakteryzując się specyficznymi wymaganiami mającymi wpływ na zarządzanie zasobami personalnymi:

- specyfika branży to regulacje i wymagania, co wymaga od pracowników przestrzegania surowych norm bezpieczeństwa i jakości, kluczowe dla pracowników są szkolenia,
- wysoka specjalizacja, certyfikacja w sektorze lotniczym, wymaga zaawansowanych systemów rekrutacji i szkoleń specjalistów z wąskich dziedzin,
- rekrutacja i selekcja poprzez wykorzystanie zaawansowanych narzędzi rekrutacyjnych, systemów do zarządzania aplikacjami, które pomagają w zbieraniu, analizowaniu i selekcjonowaniu personelu,
- zarządzanie talentami poprzez szkolenia, programy mentoringowe jest to pozyskiwanie i rozwijanie talentów w lotnictwie,
- ciągłe kształcenie poprzez regularne uczestnictwo w kursach, aby utrzymać posiadane umiejętności na odpowiednim poziomie,
- nowe technologie VR i symulatory w szkoleniu pozwalają na bezpieczne i efektywne kształcenie,
- zarządzanie wydajnością pracowników uwzględniające aspekty takie jak, jakość pracy, innowacyjność, przestrzeganie norm,
- coaching i feeadback, są niezbędne w kontekście pracy zespołowej i rozwoju osobistego,

[8] R. Birnbach, T. Longridge, *The Regulatory Perspective*, [w:] *Cockpit Resource Management*, red. E. Wiener, B. Kanki, R. Helmreich, Academic Press.San Diego 1993.

- zarządzanie różnorodnością w zespołach wielokulturowych wymaga zrozumienia pracy zespołowej,
- inclusion initiatives, to wdrażanie polityki na rzecz różnorodności i włączenia w przyciąganie talentów,
- technologie i innowacje poprzez zastosowanie systemów ERP i HRM, w celu zapewnienia spójności danych w podejmowaniu decyzji,
- analiza danych HR, do monitorowania trendów w przewidywaniu potrzeb, jak też optymalizacji procesów HR,
- zarządzanie rotacją i zatrudnieniem w analizie przyczyn odejść oraz podejmowaniu działań dla poprawy retencji w kontekście wysokich kosztów szkoleń,
- zarządzanie kryzysowe, plany awaryjne, które obejmują zarządzanie personelem w sytuacjach nagłych, nieprzewidzianych okolicznościach. Wymaga elastyczności, innowacyjności oraz nowoczesnych technologii w podejściu opartym na danych dla osiągnięcia sukcesu.

Poza pilotami, określanymi mianem ostatniego ogniwa w łańcuchu bezpieczeństwa lotniczego, niemniej istotną rolę odgrywa personel techniczny i kontrolerzy ruchu lotniczego. W dzisiejszych czasach szczególnie dużą wagę przywiązuje się do pożądanego stanu tzw. świadomości sytuacyjnej (ang. situational awareness - SA). Niezależnie od rodzaju lotnictwa branego pod uwagę (lotnictwo ogólne, bussinesowe, czy też państwowe, lotnicze pogotowie ratunkowe, lotnictwo policji, straży granicznej, sił zbrojnych) utrzymanie pożądanego stanu świadomości sytuacyjnej w odniesieniu do ww. personelu jest jednym z zasadniczych elementów decydujących o poziomie bezpieczeństwa realizacji zadań lotniczych. W branży lotniczej wyróżnia się m.in. szkolenia:

- wielozakresowe we współpracy w załodze wieloosobowej (ang. *Multi-Crew Cooperation*, MCC),
- z czynnika ludzkiego (ang. *Human Factor*, HF),
- z zarządzania zasobami ludzkimi (ang. *Crew Resource Management*, CRM),
- z zarządzania zagrożeniami i błędami (ang. *Threat and Error Management*, TEM), dotyczące zaleceń po zaistniałych zdarzeniach, incydentach czy katastrofach lotniczych,
- zapobieganie i wyprowadzanie samolotu z sytuacji krytycznych (*Upset Prevention and Recovery Training*, UPRT),
- szkolenia stanowiskowe.

Chcąc umożliwić rozwój personalny osób chętnych do pracy w lotnictwie, nie tylko w szkołach średnich, technikach, uczelniach wyższych organizowane są kursy specjalistyczne, które zachęcają ludzi bez względu na płeć do spróbowania swoich sił. Warto pamiętać, że instruktor specjalności lotniczej jest nie tylko nauczycielem zawodu, ale także wychowawcą i w trakcie każdego etapu szkolenia powinien wpajać swoim uczniom zasady etyki lotniczej, zasady bezpiecznego wykonywania operacji lotniczych, a przede wszystkim odpowiedzialności.

Trening nie może opierać się tylko na nauce teorii, musi dążyć do wytworzenia świadomości potencjalnych zagrożeń i opierać się na aktywnym działaniu mającym na celu podniesienie efektywności działań[9]. Promuje także świadomość zachowań ludzkich, poprawiając komunikację i relacje interpersonalne osób zaangażowanych w operacje lotnicze (piloci, stewardessy/stewardzi, pracownicy wieży kontroli lotów, obsługa naziemna, mechanicy). Pozwala zobaczyć szerszą perspektywę związaną z natężeniem operacji powietrznych, planowaniem załóg na lot, planowaniem szkoleń. Uświadamia także ogromną wagę odpowiedniej współpracy z firmami oraz osobami niezatrudnionymi bezpośrednio przez operatora, takimi jak straż graniczna, straż pożarna, inżynierowie, mechanicy, agenci handlingowi, obsługa check in, inspektorzy CAA[10], pracownicy cateringu, osoby odpowiedzialne za tankowanie samolotu i wiele innych.

Szkolenie kadr

Dobór kadr oraz szkolenie w każdej specjalności, to czas minimum od 1 roku do 3 lat teorii a następnie odbywanie praktyki specjalistycznej pod okiem instruktorów w ilości godzin spędzonych w powietrzu, pracy na sprzęcie czy też na stanowisku kontrolera praktykanta. To wszystko jest określone przepisami. Należy posiadać odpowiednią kategorię zdrowia. Zdanie egzaminów teoretycznych i praktycznych odbywa się przed nadzorem lotniczym. Trzeba być przygotowanym na stres i inne czynniki zewnętrzne, które nieraz stawiają priorytety. Przepisy, jak również programy ulegają ciągłym modyfikacjom. Szkolenia z zasad bhp i pracy w organizacji lotniczej oraz podstawowe

[9] J. Ślusarski, *Sztuka zarządzania zasobami własnymi oraz zespołu jako metakompetencja pilota i pilota instruktora funkcjonującego w sytuacjach trudnych i niebezpiecznych*, Annales, Vol. 30, no 2, 2017, s. 64.

[10] CAA - Civil Aviation Authority, Urząd Lotnictwa Cywilnego.

z bezpieczeństwa lotniczego muszą odbyć wszyscy pracownicy. Szkolenia specjalistyczne wiążą się z certyfikatami, upoważnieniami, licencjami lotniczymi wydawanymi przez Władzę Lotniczą. W Polsce, z ramienia Ministra infrastruktury jest nią Urząd Lotnictwa Cywilnego, zgodnie z Ustawą Prawo Lotnicze. Z ramienia Unii Europejskiej nad Urzędem nadzór sprawuje Europejska Agencja Bezpieczeństwa Lotniczego (EASA).

Koszt wykształcenia pilota w Polsce, to około 300 tyś. zł. Dlatego wielu pilotów zagranicznych ma swój epizod lotniczy w Polsce. Kształcenie może odbywać się dwuwariantowo tzn. modułowo – etapami: pierwsza licencja PPL(A), a następnie zdobywając kolejne uprawnienia do licencji zawodowej CPL(A)z nalotem 200 godzin spędzonych w powietrzu i zdanym egzaminem teoretycznym ATPL(A) „Frozen", egzaminami na poszczególne praktyczne uprawnienia lotnicze jak: IR, ME i licencję zawodową CPL(A). Drugi wariant to szkolenie zintegrowane odbywające się w jednym ciągu od zera i dopiero po zakończonym szkoleniu teoretycznym i praktycznym naprzemiennym zalicza się egzaminy ATPL(A) „Frozen" teoretyczny i egzamin praktyczny na licencję CPL(A) z uprawnieniami do lotów wg. przyrządów i na samoloty wielosilnikowe. Po tych ścieżkach można już ubiegać się o pracę w liniach lotniczych. Wielu przewoźników przedstawia wyższe kryteria, co do nalotu praktycznego na samolotach. Nalot, który odbywał się na symulatorach, nie jest uwzględniany[11].

Każdy chętny do pracy w liniach lotniczych musi przejść wieloetapową rekrutację począwszy od psychologa, poprzez zajęcia grupowe, sprawdzenie umiejętności na symulatorze oraz mieć odpowiednią kategorię zdrowia. Symulatory stają się już narzędziem pospolitym w szkołach lotniczych jako urządzenie do szkolenia procedur nawigacyjnych, ćwiczenia sytuacji awaryjnych, lotów kontrolnych na modelach samolotów do oceny kompetencji. W liniach lotniczych używa się Ful Flight Simulator do określonego typu samolotu do szkolenia na typ oraz oceny kompetencji. Kapitan jako najważniejsza osoba na pokładzie, odpowiedzialna za powierzony sprzęt i ludzi zawsze w imię dobrej praktyki powinien przeprowadzić prostą mentalną odprawę wykonaną chwilę przed startem, najlepiej wypowiedzianą na głos, co pozwoli przejść załodze przez wszystkie krytyczne zagadnienia, zanim sytuacja przyspieszy do tempa, które nie będzie komfortowe i nie zostawi miejsca na przemyślenia. Jest takie

[11] J. Kozuba, T. Compa, *Wpływ szkolenia doskonalącego załogi statku powietrznego na kształtowanie świadomości sytuacyjnej*, Logistyka, nr 3, 2012, s. 1152.

piękne angielskie powiedzenie lotnicze: „A superior pilot uses his superior judgment to avoid situations which require the use of his superior skill.", które idealnie wpisuje się w tę logikę bycia przygotowanym[12].

Szkolenie z wiedzy teoretycznej mechaników lotniczych obejmuje wszystkie dziedziny i zgodnie z programem studiów – wykłady i ćwiczenia – specjalność płatowce, silniki lotnicze, wyposażenie pokładowe. Należy potwierdzić obecność (1 000 godzin zegarowych) na wykładach i ćwiczeniach z przedmiotów, które są ujęte w programie kształcenia. Następnie szkolenie praktyczne zgodne z programem studiów – laboratoria i ćwiczenia- specjalność płatowce, silniki, osprzęt lotniczy. Należy potwierdzić obecność na zajęciach teoretycznych i uzyskać pozytywną ocenę (416 godzin zegarowych) na zajęciach laboratoryjnych i ćwiczeniach, które są ujęte w programie szkolenia uczelni. Dla przykładu praktyczne szkolenie obsługowe we wskazanej przez uczelnię organizacjach obsługi technicznej. Należy potwierdzić obecność i uzyskać pozytywną ocenę (540 godzin zegarowych) na praktycznych szkoleniach obsługowych, które są ujęte w programie szkolenia praktycznego.

Należy zdać egzaminy z wiedzy teoretycznej – 13 - 17 modułów między innymi: z techniki lotniczej, czynnika ludzkiego i przepisów lotniczych, w zależności od specjalizacji. Po każdym zdanym egzaminie z wiedzy teoretycznej, wystawiany jest odpowiedni Certyfikat z każdego modułu. Dodatkowo (poza certyfikowanym szkoleniem) musi być odbyta roczna praktyka obsługowa w dowolne,j certyfikowanej zgodnie z Part-145 lub Part-M/F – organizacji obsługi technicznej samolotów. Praktyka obsługowa musi być potwierdzona w książce mechanika przez organizację. Sukcesem jest osiągnięcie licencji mechanika lotniczego obsługi EASA PART – 66.

Podpisanie umowy o współpracy pomiędzy Uczelnią a LOT Aircraft Maintenance Serrvices (LOTAMS) będzie dotyczyć pozyskiwania i realizacji projektów B+R+W, rozwoju kompetencji kadry naukowo – technicznej, studentów, dostosowania programów studiów, laboratoriów dydaktyczno – badawczych do profilu działalności LOTAMS oraz praktyk i staży studentów[13].

[12] Ł. Wieczorek, *Fly-Navigate–Communicate, czyli podział obowiązków przed lotem w załodze wieloosobowej*, 18.02.2025, dlapilota.pl, https://dlapilota.pl/wiadomosci/polska/artykul-z-nagroda-fly-navigate-communicate-czyli-podzial-obowiazkow-przed-lotem-w, [dostęp: 18.02.2025].

[13] *Politechnika Rzeszowska podpisała umowę z LOTAMS*, Politechnika Rzeszowska im. Ignacego Łukasiewicza, https://w.prz.edu.pl/uczelnia/aktualnosci/politechnika-rzeszowska-podpisala-umowe-z-lotams-1541.html, [dostęp: 11.04.2015].

Przed uczelniami wyższymi stoją nowe wyzwania. Tworzone są nowe specjalności w kształceniu kadr dla branży lotniczej od konstruktora, informatora FIS, kontrolera ruchu lotniczego poprzez Marshallera, mechanika lotniczego, stewardessę, pilota, do najwyższych stanowisk w zarządzaniu działem i firmą lotniczą, bez względu czy produkującą, czy też świadczącą usługi w biznesie lub w transporcie pasażerów[14].

Podniebna przygoda – stewardessa. W tym zawodzie liczy się zadbany wygląd i dobra prezencja. Stewardessa musi mieć odpowiednie umiejętności, wymuszone przez sam charakter zawodu. Dobra organizacja pracy, punktualność, komunikatywność i odporność na stres — to tylko niektóre z nich. Od osób ubiegających się o pracę w zawodzie stewardesy i stewarda wymagany jest:

- wiek najczęściej do 30 lat,
- schludny wygląd i zgrabna sylwetka,
- wykształcenie min. średnie (niektóre linie wymagają wyższego wykształcenia), dobra znajomość języków obcych - angielski obowiązkowo oraz najlepiej jeszcze co najmniej jeden, inny język europejski,
- umiejętność pływania - w przypadku awaryjnego lądowania załoga musi zadbać o bezpieczeństwo swoje i pasażerów (na kursie dla stewardess będziesz się uczyć zachowania w razie wodowania, sposobów przetrwania w wodzie, holowania ludzi),
- wzrost 160-170 cm w przypadku kobiet i 170-180 cm w przypadku mężczyzn (chociaż każda firma podaje najczęściej swoje indywidualne wymogi odnośnie do wzrostu),
- brak cukrzycy i migreny,
- niektóre firmy nie przyjmują osób z wadą wzroku większą niż – 3 dioptrie (ewentualnie kandydat może nosić szkła kontaktowe, okulary dyskwalifikują). Dyskwalifikowani są kandydaci z tatuażami w widocznym miejscu oraz z kolczykami na twarzy (to zależy od linii lotniczych),
- dla przykładu: kandydaci na stewardessy i stewardów, którzy ubiegali się o pracę w Wizz Air, musieli mieć przynajmniej 19 lat, stewardessy musiały mieć co najmniej 165 cm wzrostu, a stewardzi – 175 cm,
- kandydaci mogą też spodziewać się zadań sprawdzających refleks, scenek symulujących sytuacje awaryjne czy konfliktowe oraz pytań o reakcję

[14] *Istambuł pierwszym w Europie lotniskiem z systemem umożliwiającym jednoczesny start trzech samolotów*, dlapilota.pl, https://dlapilota.pl/wiadomosci/swiat/istambul-pierwszym-w-europie-lotniskiem-w-systemem umozliwiajacym-jednoczesny, [dostęp: 15.04.2025].

w konkretnych przypadkach np. w lotach do krajów afrykańskich czy też azjatyckich.

Szkolenie rozpoczyna się od elementarza Flight Attendant Manual, czyli po prostu podręcznika dla personelu pokładowego. Jest to podstawowy dokument w każdej linii lotniczej. To pierwsze i najważniejsze źródło wiedzy o zasadach pracy stewardessy i stewarda - od procedur bezpieczeństwa, po sposób serwowania posiłków pasażerom w klasie biznesowej. Potem, już w czasie zajęć, zostają przedstawione procedury: bezpieczeństwa na pokładzie samolotu, ewakuacji pasażerów w razie sytuacji niebezpiecznych, medyczne i ratunkowe (w tym, tzw. „pierwsza pomoc"), serwisowe, tzw. grooming, czyli profesjonalny makijaż i sposób odgrywania roli „modela" firmy, również trzeba uczyć się prawa lotniczego. Szkolenie zawsze kończy się egzaminem z teoretycznym i praktycznym Cabin Crew.

Chcąc umożliwić rozwój personalny osób chętnych do pracy w lotnictwie, nie tylko w szkołach średnich, technikach, uczelniach wyższych organizowane są kursy specjalistyczne, które zachęcają ludzi bez względu na płeć, do spróbowania swoich sił. Warto pamiętać, że instruktor specjalności lotniczej jest nie tylko nauczycielem zawodu, ale także wychowawcą i w trakcie każdego etapu szkolenia powinien wpajać swoim uczniom zasady etyki lotniczej, zasady bezpiecznego wykonywania operacji lotniczych, a przede wszystkim odpowiedzialności. Kontrolerzy Ruchu Lotniczego zapewniają bezpieczeństwo załogom i pasażerom statków powietrznych w czasie lotu i manewrowania po lotnisku, pilnują uporządkowanego i sprawnego utrzymywania przepływu ruchu lotniczego, jak również zapobiegania niebezpiecznym zbliżeniom w powietrzu, separacji między statkami powietrznymi w przestrzeni kontrolowanej poprzez wydanie odpowiednich zezwoleń i instrukcji dotyczących lotów, poprzez utrzymywanie dwustronnej łączności.

W Polsce pracuje na stanowisku kontrolera około 540 licencjonowanych kontrolerów. Najnowsze prognozy długoterminowe wskazują, że do 2040 r. ruch lotniczy w europejskiej przestrzeni powietrznej wzrośnie do nieco ponad 44 000 lotów dziennie, co oznacza całkowity wzrost do około 53% dziennej liczby operacji lotniczych. Oznacza to, że znaczna część zapotrzebowania na loty może nie zostać uwzględniona. Inną ważną kwestią do rozważenia, która w tym przypadku jest faktycznym przedmiotem zainteresowania, jest wpływ obecnej sytuacji w europejskiej przestrzeni powietrznej na efektywność lotów.

Ten czynnik jest szczególnie ważny zarówno dla podmiotów ATM[15], jak i użytkowników przestrzeni powietrznej, takich jak operatorzy linii lotniczych.

Kobiety w lotnictwie

Kobiety w lotnictwie odgrywają coraz ważniejszą rolę, zarówno w zakresie pilotowania statków powietrznych, mechaników technicznych oraz obszarach menedżerskich.

Coraz bardziej zajmują miejsce przeznaczone dla mężczyzn, przełamując bariery społeczne, stając się ikonami lotnictwa. Wyszły zza biurek. Są przy odprawach pasażerów. Coraz więcej Pań widzimy w mundurach kapitanów. Programy takie jak WASP[16] w USA, umożliwiły kobietom pilotowanie samolotów wojskowych. Pod względem liczby kobiet pilotów, w rankingu przodują Stany Zjednoczone oraz Kanada. Procentowo, spośród amerykańskich przewoźników, największy udział kobiet za sterami samolotów, 9,6 proc., mają linie lotnicze Hawaiian Air. Spośród „Amerykańskiej wielkiej trójki" na czoło rankingu wysuwają się linie lotnicze United Airlines, gdzie 7,5 proc. załóg personelu kokpitowego stanowią kobiety. Na kontynencie amerykańskim, najmniej kobiet zasiada za sterami przewoźników niskokosztowych. W liniach lotniczych Southwest Airlines oraz Allegiant Air kobiety stanowią 4,1 proc. ogółu załóg, podczas gdy w Spirit Airlines jedynie 3,1 proc. Polki też nie odpuszczają. W LS Airport Services pracują we wszystkich obszarach spółki: w terminalach pasażerskich, na płycie lotniska czy magazynach cargo. Pełnią różnorodne funkcje - od koordynatora rejsów, kierowcy busa premium, poprzez agentów obsługi pasażerskiej, obsługę PRM, wyposażanie i sprzątanie pokładów samolotów, po funkcje kierownicze i dyrektorskie. Prezesem zarządu LOTAMS jest Ewa Kołowiecka[17].

Profilaktyka

Należy pamiętać o ogólnej zasadzie lotnictwa: „Za całość bezpieczeństwa lotu, wszystkie jego aspekty od chwili wejścia na pokład do jego opuszczenia odpowiada osobiście pilot dowodzący statkiem powietrznym.

[15] ATS – Air Traffic Services, Służby Ruchu Lotniczego.

[16] WASP – Women Airforce Service Pilots.

[17] *Nowa prezes i członek zarządu w LOTAMS*, Rynek Lotniczy, https://www.rynek-lotniczy.pl/wiadomosci/nowa-prezes-i-czlonek-zarzadu-w-lotams-22777.html, [dostęp: 11.04.2025].

Czynnik ludzki w całym łańcuchu jest najsłabszym ogniwem. Problemy, które uwidoczniły się w badaniach zdarzeń, katastrof lotniczych spowodowanych współpracą w kokpicie, świadomością sytuacyjną, operacyjną, przełożyły się na dodatkowe szkolenie, doszkalanie załóg poprzez zajęcia teoretyczne online oraz w „ławce", jak również praktyczne w czasie sesji symulatorowych. Uwzględniono te niedociągnięcia w szkoleniach już na etapach szkoleń podstawowych do licencji i uprawnień do nich wpisywanych. Szkolenia te muszą być odświeżane, co do typu samolotu, u przewoźnika lotniczego[18].

Ważnym aspektem dotyczącym problemu bezpieczeństwa jest sposób wykonywania czynności służbowych przez służby w porcie lotniczym, kokpicie samolotu, czy też na wieży. Nie jest niczym nowym stwierdzenie, że człowiek popełnia błędy. Ich popełnienie jest tylko kwestią czasu, nawet dla perfekcyjnego pracownika. Stwierdzenie to właściwie jest uzupełnieniem statystyk, protokołów pokontrolnych, raportów z badań wypadków lotniczych, mówiących o niewłaściwym postępowaniu załogi i skutkach ich działań. Istotnym kryterium w pracy jest przygotowanie do wykonania zadania, koncentracja, wystarczy chwila nieuwagi, zajęcie dyskusją na inny temat, a spowoduje to stratę czasu i przestrzeni. O fatalnej pomyłce dowiadujemy się po czasie. Po raz kolejny widzimy, że to człowiek jest najsłabszym, ułomnym ogniwem w łańcuchu bezpieczeństwa lotniczego.

Obowiązujące procedury w porcie lotniczym są wdrażane w celu usprawnienia i ułatwienia pasażerom i pracownikom kontroli bezpieczeństwa czynności obowiązujących w trakcie kontroli przed wejściem do strefy zastrzeżonej portu lotniczego, a następnie na pokład samolotu. Wspólne zaufanie w branży tylko ułatwi pracę, ale spowoduje, że błędy staną się tylko symboliczne, ponieważ zostaną wychwycone już na początku. Stąd też tak ważne jest, aby we wszelkie szkolenia był włączony czynnik z budowy świadomości, który jest dzisiaj najważniejszy w systemie zarządzania bezpieczeństwem, w tym również ochrony w eliminacji zagrożeń.

Zarządzanie zagrożeniami i błędami (TEM)[19] jest nadrzędnym podejściem do zarządzania bezpieczeństwem w transporcie lotniczym. W oparciu o badanie wypadków lotniczych regularnego transportu zostały opracowane ramy TEM przez psychologów z University of Texas, celem zidentyfikowania

[18] Z. Ciekanowski, Z. Piskor, *System kontroli bezpieczeństwa w transporcie lotniczym w Polsce w latach 2015– 2022*, MANS, Warszawa 2024, s. 170.

[19] Latajmy Bezpiecznie: CRM – TEM – HF, https://dlapilota.pl/wiadomosci/latajmy-bezpiecznie/latajmy-bezpiecznie-crm-tem-hf, [dostęp: 22.04.2025].

zagrożenia i błędów podczas wykonywania operacji lotniczych. Posłużył temu audyt bezpieczeństwa (LOSA) wykonany przez obserwatora, a obejmujący identyfikację, gromadzenie informacji z zagrożeniami w operacjach związanych z bezpieczeństwem, w tym warunków środowiskowych, złożoności operacyjnej, wydajności załóg. Dane z audytów są wykorzystywane do oceny organizacji, w jaki sposób procedury są wdrażane i wykonywane w bieżących operacjach.

Procedury bezpieczeństwa, listy kontrolne, jakie są używane w kokpitach samolotów, jak również audytorów i inspektorów nadzorów lotniczych istnieć będą, ale ulegają ciągłym zmianom, modyfikacjom, chociażby z powodów cyberprzestępczości, terroryzmu, zmian przepisów i regulacji prawnych. Lotniska, przewoźnicy, organizacje lotnicze cały czas wprowadzają ułatwienia w uzgodnieniu z nadzorami lotniczymi, a także z EASA i ICAO, podejmując działania legislacyjne: rozporządzenia, wytyczne, standardy, procedury, instrukcje. W tym celu kierownictwo organizacji powinno stwarzać odpowiednie warunki pracy, zapewniając wysoki poziom szkolenia załogi, nadzór wewnętrzny, niezbędną bazę materiałowo-techniczną.

Tylko systemowe promowanie i łączenie najlepszych praktyk w każdej z dziedzin i obszarów lotnictwa cywilnego ma szczególne znaczenie w podnoszeniu świadomości poprzez zaplanowane działania wespół z organizacjami innych krajów i organizacji międzynarodowych jak EASA, ICAO. Stąd rok 2020/2021 ustanowiony był Rokiem Kultury Ochrony Lotnictwa Cywilnego[20] przez Międzynarodową Organizację Lotnictwa Cywilnego.

Zagrożenia bezpieczeństwa lotniczego są ciągle przedmiotem badań wielu dziedzin nauki. Ich celem jest poszukiwanie rozwiązań zmniejszających ryzyko związane z wykonywaniem operacji i unikanie związanych z tym strat. Awarie i wypadki w transporcie lotniczym często są skutkiem niebezpiecznych zachowań, dlatego należy:

- promować bezpieczeństwo,
- zachęcać do stosowania nowych narzędzi m.in. symulatorów, w celu wyeliminowania luki czasowej, budować bazę wiedzy o zdarzeniach, aby zapobiegać analogicznym zdarzeniom w przyszłości,
- wdrażać własne propozycje wspierania bezpieczeństwa, mające wpływ na podnoszenie jakości szkolenia w organizacji,

[20] Year of Security Culture 2021, ICAO, https://www.icao.int/Security/Security-Culture/Pages/YOSC-2021.aspx, [dostęp: 7.04.2025].

- inicjować skuteczne działania następcze i zapobiegawcze,
- proaktywnie wprowadzać złożone i skuteczne bariery bezpieczeństwa, nieustannie doskonalić ogólny system zarządzania i SMS,
- dokonywać weryfikacji procedur operacyjnych,
- minimalizować ryzyko HF,
- zmieniać profil ryzyka i ograniczać podatność,
- zapewnić dostateczne zasoby wykwalifikowanej kadry (piloci, kontrolerzy, mechanicy, inżynierowie lotniczy, menedżerowie),
- zapewnić większą gęstość lotnisk przystosowanych do lotów instrumentalnych w Polsce, która jest zbyt mała w stosunku do sieci lotnisk w krajach Europy Zachodniej.

Powstają nowe stanowiska, gałęzie w przemyśle lotniczym, do których potrzeba specjalistów z dziedziny IT w zarządzaniu systemami i koordynowaniu działań w rozwiązywaniu zaistniałych newralgicznych sytuacji na ziemi.

Podsumowanie

Przemysł lotniczy jest kluczowy dla gospodarki narodowej, a inwestycje w rozwój technologii i innowacji są niezbędne, aby sprostać rosnącym wymaganiom rynku oraz wyzwaniom związanym ze zrównoważonym rozwojem branży lotniczej. Załącznik 19 ICAO wskazuje nam, że bezpieczeństwo w lotnictwie jest stawiane na pierwszym miejscu[21]. Według prognoz Międzynarodowego Zrzeszenia Przewoźników Powietrznych IATA transport lotniczy kreuje i przyspiesza procesy globalizacji.

Wraz z technologią informacyjną określany jest mianem fundamentu i filaru podstawy, przy czym sam tym procesom podlega. Nowe technologie wiążą się z koniecznością zabezpieczenia przed cyberatakami. Społeczne synonimy definiowane jako branżowy zestaw wartości, odczuć, przekonań, a także zachowań organizacji i w organizacji odnoszących się do problemu bezpieczeństwa. Muszą się opierać na wysokim poziomie szacunku, zaufania na linii: przełożony - podwładny. Działania te powinny sprowadzać się do pragmatycznych formuł w zakresie kultury elastyczności, sprawiedliwego traktowania, raportowania i uczenia się. W miarę jak lotnictwo staje się bardziej zróżnicowane, można oczekiwać, że liczba kobiet w lotnictwie będzie

[21] ZDG TOR Zatrudnienie w lotnictwie. Edukacja jako odpowiedź na potrzeby branży - Rynek Lotniczy, https://www.rynek-lotniczy.pl/zdg-tor-zatrudnienie-w-lotnictwie-edukacja-jako-odpowiedz-na-potrzeby-branzy.html, [dostęp: 7.04.2025].

rosła, a ich wkład będzie doceniany. Kobiety nie tylko przyczyniają się do rozwoju lotnictwa, ale inspirują nowe pokolenia do podjęcia kariery w branży lotniczej.

Należy pamiętać o ogólnej zasadzie lotnictwa: „Za całość bezpieczeństwa lotu, wszystkie jego aspekty od chwili wejścia na pokład do jego opuszczenia odpowiada osobiście pilot dowodzący statkiem powietrznym". Czynnik ludzki w całym łańcuchu jest najsłabszym ogniwem. Powstają nowe stanowiska, gałęzie w przemyśle lotniczym, do których potrzeba specjalistów z dziedziny IT. Specjaliści będą budować samoloty, markę nie tylko firmy, ale kraju, w globalnym świecie. Wprowadzenie i rozwój szkoleń doprowadziło do potwierdzenia faktu, że bezpieczeństwo i przepustowość portu lotniczego może zostać uzyskana jedynie poprzez pracę zespołową załogi.

Literatura

1. Annual Safety Review 2023, EASA.
2. Birnbach R., Longridge T., *The Regulatory Perspective*, w: E. Wiener, B. Kanki i R. Helmreich (red.) *Cockpit Resource Management*, Academic Press.San Diego 1993.
3. Ciekanowski Z., Piskor Z., *System kontroli bezpieczeństwa w transporcie lotniczym w Polsce w latach 2015-2022*, Wydawnictwo im. prof. Leszka J. Krzyżanowskiego Menedżerskiej Akademii Nauk Stosowanych w Warszawie, Warszawa 2024.
4. Gałązkowski R., Tomaszewski M., *Bezpieczeństwo lotów a szkolenie w zakresie zarządzania zasobami załogi w zarobkowym przewozie lotniczym*, „Zeszyty Naukowe AON nr 2(99), 2015.
5. *Istambuł pierwszym w Europie lotniskiem z systemem umożliwiającym jednoczesny start trzech samolotów*, dlapilota.pl, https://dlapilota.pl/wiadomosci/swiat/istambul-pierwszym-w-europie-lotniskiem-w-systemem umozliwiajacym-jednoczesny
6. Kozuba J., Compa T., *Wpływ szkolenia doskonalącego załogi statku powietrznego na kształtowanie świadomości sytuacyjnej*, Logistyka, nr 3, 2012.
7. Latajmy Bezpiecznie: CRM – TEM – HF, https://dlapilota.pl/wiadomosci/latajmy-bezpiecznie/latajmy-bezpiecznie-crm-tem-hf
8. Liszkowska W., *Zarządzanie zasobami załogi, czyli jak uniknąć błędów zarządczych*, Zeszyty Naukowe. Organizacja i Zarządzanie, nr 71(1222), 2018.
9. *Nowa prezes i członek zarządu w LOTAMS*, Rynek Lotniczy, https://www.rynek-lotniczy.pl/wiadomosci/nowa-prezes-i-czlonek-zarzadu-w-lotams-22777.html
10. Orlandy, H.W. i H.C. Foushee, *Cockpit Resource Management Training,* Technical Report Number NASA CP-2455, Moffett Field: NASA-Ames Research Center 1987.
11. *Politechnika Rzeszowska podpisała umowę z LOTAMS*, Politechnika Rzeszowska im. Ignacego Łukasiewicza, https://w.prz.edu.pl/uczelnia/aktualnosci/politechnika-rzeszowska-podpisala-umowe-z-lotams-1541.html.

12. Urząd Lotnictwa Cywilnego, http://www.ulc.gov.pl.
13. Ślusarski J., *Sztuka zarządzania zasobami własnymi oraz zespołu jako metakompetencja pilota i pilota instruktora funkcjonującego w sytuacjach trudnych i niebezpiecznych*, Annales, Vol. 30, no. 2, 2017.
14. Wieczorek Ł., *Fly-Navigate–Communicate, czyli podział obowiązków przed lotem w załodze wieloosobowej*, 18.02.2025, dlapilota.pl, https://dlapilota.pl/wiadomosci/polska/artykul-z-nagroda-fly-navigate-communicate-czyli-podzial-obowiazkow-przed-lotem-w.
15. Year of Security Culture 2021, ICAO, https://www.icao.int/Security/Security-Culture/Pages/YOSC-2021.aspx.
16. ZDG TOR Zatrudnienie w lotnictwie. Edukacja jako odpowiedź na potrzeby branży - Rynek Lotniczy, https://www.rynek-lotniczy.pl/zdg-tor-zatrudnienie-w-lotnictwie-edukacja-jako-odpowiedz-na-potrzeby-branzy.html.

mgr Martyna Zaroślak
ORCID: 0000-0001-7693-8327
https://doi.org/10.29316/9788368103199_17

COMMERCIAL SHARENTING JAKO ZAGROŻENIE DOBROSTANU DZIECKA

COMMERCIAL SHARENTING AS A THREAT TO CHILD WELL-BEING

Streszczenie

Celem rozdziału jest analiza zjawiska commercial sharentingu jako potencjalnego zagrożenia dla dobrostanu dziecka w kontekście współczesnej cyfryzacji życia społecznego. We wstępie scharakteryzowano przemiany związane z dzieleniem się treściami dotyczącymi dzieci, od tradycyjnych form po media społecznościowe. Następnie wyjaśniono pojęcie sharentingu, ukazując jego definicje, typologie oraz różne motywacje rodziców podejmujących tego rodzaju aktywność. W kolejnej części opisano zjawisko influencer marketingu, przedstawiając sposoby zarabiania na treściach oraz wpływ tego sektora na wizerunek dzieci w sieci. Szczegółowo opisano commercial sharenting jako formę uzyskiwania korzyści materialnych z życia dziecka oraz przybliżono, jakie strategie stosują rodzice w celu zwiększenia atrakcyjności publikowanych treści. W dalszej części poddano krytycznej analizie problem kidfluencingu i wynikających z niego zagrożeń dla dzieciństwa, prywatności i rozwoju emocjonalnego małoletnich. W ostatniej

Summary

The aim of the chapter is to analyze the phenomenon of commercial sharing as a potential threat to the well-being of the child in the context of the contemporary digitization of social life. In the introduction, the transformations related to the sharing of content related to children, from traditional forms to social media, are characterized. Next, the concept of sharenting is explained, showing its definitions, typologies and various motivations of parents undertaking this type of activity. The next part describes the phenomenon of influencer marketing, presenting the ways of making money on content and the impact of this sector on the image of children online. Commercial sharenting as a form of obtaining material benefits from the child's life is described in detail and what strategies parents use to increase the attractiveness of the published content is discussed. In the next part, the problem of kidfluencing and the resulting threats to childhood, privacy and emotional development of minors were critically analyzed. The last part of the chapter introduces

części rozdziału przybliżono kwestie regulacji prawnych, omawiając przepisy obowiązujące w Polsce i innych państwach oraz wskazując na istniejące luki prawne. Problem badawczy sformułowano: czy wykorzystywanie wizerunku dzieci w mediach społecznościowych w celach zarobkowych rzeczywiście stanowi zagrożenie dla ich praw i bezpieczeństwa? W rozdziale zastosowano odpowiednie metody badawcze. W szczególności dokonano analizy literatury przedmiotu, w tym dokumentów prawnych, raportów i badań naukowych, przeanalizowano również zjawiska społeczne i trendy medialne oraz poddano krytycznej ocenie istniejące regulacje prawne.

Słowa kluczowe: sharenting, kidfluencer, prawa dziecka, influencer marketing, ochrona prywatności

the issues of legal regulations, discussing the regulations in force in Poland and other countries and pointing out the existing legal loopholes. The research problem was formulated: does the use of children's images on social media for commercial purposes really pose a threat to their rights and safety? Appropriate research methods were used in the chapter. In particular, the literature on the subject, including legal documents, reports and scientific research, social phenomena and media trends were also analyzed, and the existing legal regulations were critically evaluated.

Keywords: sharenting, kidfluencer, children's rights, influencer marketing, privacy protection

Wstęp

Dzielenie się fotografiami własnych dzieci nie jest zjawiskiem nowym – rodzice, choć od zawsze pokazywali innym momenty z życia ich pociech, jeszcze kilkanaście lat temu wykonywali to na dużo mniejszą skalę. Wraz z rozwojem technologii tradycyjne rodzinne albumy i pokazy slajdów, które kiedyś były przeznaczone tylko dla wąskiej publiczności członków rodziny i przyjaciół, zostały zastąpione przez platformy społecznościowe docierające do nieporównywalnie większej liczby osób, w tym osób nieznajomych. Znacząco zmienił się sposób również tworzenia i udostępniania treści dowolnego rodzaju – fotografia cyfrowa, smartfony i media społecznościowe wzmocniły więc zachowanie, które już istniało, umożliwiając po prostu dzielenie się fotografiami dzieci na nieporównywalnie większą skalę.

Obecnie zarówno influencerzy, jak i zwykli użytkownicy na całym świecie dokumentują swoje życie w mediach społecznościowych. Dobierając publikowane treści tak, aby przyciągnęły zainteresowanie odbiorców, tworzą w cyfrowym świecie zainscenizowaną wersję siebie. W centrum tych działań coraz częściej jako element medialnego przekazu znajduje się dziecko. Starannie przygotowane posty, selekcja najkorzystniejszych materiałów czy cyfrowe poprawianie zdjęć przed ich opublikowaniem, to zachowanie widoczne

u rodziców, którzy inscenizują fotografie swoich dzieci w sposób mający zapewnić im osiągnięcie pewnych korzyści

Zjawisko określane mianem sharentingu zyskało szczególną intensywność i nowy, komercyjny wymiar. Wraz z dynamicznym rozwojem influencer marketingu pojawiła się praktyka commercial sharentingu, w której wizerunek dziecka jest wykorzystywany w celach zarobkowych.

Sharenting – zarys definicji

Termin sharenting powstał z połączenia dwóch angielskich słów – share (rozpowszechniać) i parenting (rodzicielstwo). Po raz pierwszy pojawił się prawdopodobnie w 2012 roku, w jednym z artykułów opublikowanych przez Wall Street Journal, dotyczącym rodziców starających się zwrócić na siebie uwagę w Internecie nadmiernie dzieląc się informacjami o swoich dzieciach[1].

Internetowy Słownik Collinsa definiuje zjawisko jako „zwyczajowe korzystanie z mediów społecznościowych w celu udostępniania wiadomości, zdjęć itp. swoich dzieci”[2]. Określenie ‘zwyczajowe’ może sugerować, że jest to działanie powtarzalne. Ta nieformalna definicja jest dość ogólna, uszczegóławia ją Phoebe Maltz Bovy, wymieniając dwa kryteria, które muszą zostać spełnione, aby mówić o zjawisku sharentingu: obecność masowej publiczności i możliwość identyfikacji dziecka[3]. Natomiast Anna Brosch dodaje jeszcze jeden istotny czynnik – potencjalne ryzyko dla dzieci. Idąc za tym rozumowaniem definiuje ona sharenting jako „upublicznianie przez rodziców wielu szczegółowych informacji o swoich dzieciach w postaci zdjęć, filmów i postów za pośrednictwem mediów społecznościowych, które naruszają prywatność dzieci”[4].

[1] M. N. Fineman, *Honey, I Monetized the Kids: Commercial Sharenting and Protecting the Rights of Consumers and the Internet's Child Stars*, The Georgetown Law Journal, t. 11, nr 4, 2023, s. 848-849.

[2] *SHARENTING definition and meaning | Collins English Dictionary*, https://www.collinsdictionary.com/dictionary/english/sharenting, [dostęp: 10.04.2025].

[3] A. Brosch, *Sharenting – Why Do Parents Violate Their Children's Privacy?*, The New Educational Review, t. 54, 2018, s. 78.

[4] Ibidem, s. 78.

Stopień, w jakim rodzic angażuje się w sharenting, jest mierzony według czterech elementów: ilości publikowanych treści, częstotliwości tego działania, rodzaju udostępnianych informacji i liczebności odbiorców[5].

Sharenting oferuje rodzicom wiele korzyści, między innymi możliwość rozwijania tożsamości rodzicielskiej, utrzymywanie relacji społecznych i rodzinnych, otrzymywanie wsparcia, informacji i wskazówek czy możliwość dyskusji na temat doświadczeń rodzicielskich w domenie publicznej.

Pod względem aktywności rodzica można go sklasyfikować na trzy główne typy[6]:

- aktywny (gdy rodzice działają celowo, nawet jeśli nie są świadomi możliwych konsekwencji);
- pasywny (działanie niezamierzone – może mieć miejsce, gdy posty są wtórnie udostępniane przez inne osoby);
- niewidoczny (gdy rodzice dzielą się nieświadomie informacjami z firmami komercyjnymi).

Różne typy mogą występować razem – treści publikowane celowo mogą być udostępniane przez innych użytkowników, jednocześnie pośrednio przekazując informacje specjalistom od marketingu.

Influencer marketing: praktyki zarobkowe w mediach społecznościowych

Influencerzy w mediach społecznościowych to „podzbiór twórców treści cyfrowych zdefiniowanych przez ich znaczącą liczbę obserwujących w Internecie, charakterystyczną osobowość marki i wzorcowe relacje ze sponsorami komercyjnymi”[7]. Określenie ‘twórca treści’ sugeruje nacisk na kreatywny aspekt tworzenia w celu zaangażowania odbiorców.

Rozróżnienie terminologii jest istotne, ponieważ nie wszyscy twórcy treści są influencerami (nawet jeśli gromadzą polubienia i obserwujących), ale wszyscy influencerzy są w istocie twórcami treści. Można więc założyć, że influencerzy to wysoce profesjonalni twórcy treści, którzy mogą kształtować

[5] Ibidem, s. 79-80.

[6] A. Ruiz-Gómez, *Commercial Sharenting on Instagram: How Parents Build Social Capital and Monetize Baby Accounts Sharenting. Tesis doctoral, Universidad Complutense De Madrid*, Madrid 2023, s. 110.

[7] Ibidem, s. 66.

opinie nabywców konsumenckich, czyli poniekąd wywierać wpływ na swoją społeczność obserwujących[8].

Media społecznościowe już kilka lat temu zmieniły swoje praktyki marketingowe i zaczęły wykorzystywać influencerów jako pośredników łączących ich marki z potencjalnymi konsumentami. Twórcy, którzy skutecznie przyciągają odbiorców, mogą zarabiać na życie promując produkty i usługi obserwującym ich użytkownikom.

Istnieją dwa główne sposoby na otrzymywanie wynagrodzenia za tworzone przez influencerów treści[9]:

- jako płatności z platform mediów społecznościowych, gdy witryna przekazuje przychody z reklam umieszczanych przez osoby trzecie w treściach twórców;
- jako bezpośrednie sponsorowanie, gdy reklamodawcy zawierają umowy bezpośrednio z twórcami, w celu płacenia za posty promujące ich produkty.

W przypadku pierwszego rodzaju wynagrodzenia każdy z serwisów administruje płatnościami na własny sposób.

Według corocznego rankingu Forbes zarobki mega influencerów (twórców, którzy mają ponad milion obserwujących) wahają się od 16 milionów do 54 milionów dolarów rocznie, a pod względem powszechnego uznania publicznego mogą oni konkurować z tradycyjnymi celebrytami[10]. Niektórzy influencerzy mają domy wypełnione darmowymi przedmiotami – od markowych ubrań, przez meble, po nowoczesne sprzęty. Część z rzeczy pochodzi ze współpracy barterowych – umów, w których „wykonawca usługi nie dostaje w zamian pieniędzy, lecz towar lub inną usługę, np. tablet, komplet ubrań, wakacyjny wyjazd czy wizytę w salonie piękności”[11].

W 2024 roku media społecznościowe stały się największym kanałem reklamowym na świecie, a wielkość rynku influencerów w branży reklamowej

[8] Ibidem, s. 66-67.

[9] C. Yates, *Influencing„Kidfluencing”: Protecting Children by Limiting the Right to Profit From „Sharenting”*, Vanderbilt Journal of Entertainment & Technology Law, t. 25, nr 4, 2023, s. 864.

[10] A. Ruiz-Gómez, *Commercial Sharenting ...,* op. cit., s. 69-71.

[11] *Rodzinka w barterze. Weszliśmy za kulisy biznesu opartego na dzieciach*, https://spidersweb.pl/plus/2023/06/instagram-rodzice-dzieci-barter-wspolpraca-reklama-zarobki, [dostęp: 11.04.2025].

wyniosła 24 miliardy dolarów. Szacuje się, że w 2025 roku kwota ta wzrośnie do 32,55 miliarda dolarów[12].

Influencer marketing to technika marketingowa opisywana jako „rodzaj reklamy natywnej, w której marki wykorzystują influencerów w mediach społecznościowych do promowania produktów lub usług wśród swoich obserwujących, w zamian za wynagrodzenie"[13]. Reklamodawcy oczekują, że influencerzy będą osadzać treści promocyjne w bezpłatnych dla innych użytkowników treściach, aby dotrzeć do odbiorców w bardziej subtelny sposób. Tegu typu kampanie są uważane za skuteczne i opłacalne, gdyż konsumenci nie zawsze postrzegają płatne promocje połączone z treściami darmowymi jako reklamę.

Ponadto influencerzy są postrzegani jako postacie, z którymi można się utożsamiać, które są bardziej godne zaufania niż aktorzy występujący w tradycyjnych formach reklamy. Różne firmy wykorzystują więc zaufanie i więzi emocjonalne, które influencerzy budują ze swoimi obserwującymi[14].

Skuteczna działalność promocyjna influencerów może wynikać z następujących elementów[15]:

- wiarygodność – opinie ulubionych twórców internetowych są dla ich obserwatorów bardziej wiarygodne niż tradycyjne reklamy;
- zaufanie – relacja influencera i obserwatora opiera się na sympatii i zaufaniu, które mogą przenieść się na promowaną markę, produkt lub usługę;
- aktywność – obserwatorzy są zaangażowani w opinie zwrotne i wzajemne polecanie lub odradzanie promowanej marki, produktu lub usługi;
- atrakcyjność – influencerzy zwykle reklamują produkty lub usługi w formie recenzji, w estetyczny i dopracowany sposób;
- dopasowanie do grupy docelowej – promowane produkty lub usługi są dostosowane do potrzeb grupy odbiorczej.

Twórcy zarabiają głównie poprzez płatny sponsoring i artykuły sponsorowane, w ramach, których w swoich treściach promują produkty lub usługi lub działają jako przedstawiciele marki. Wynagrodzenie nie musi być pieniężne – inne formy wynagrodzenia obejmują prezenty lub usługi, bezpłatne

[12] I. M. Hub, *Influencer Marketing Benchmark Report 2025*, https://influencermarketinghub.com/influencer-marketing-benchmark-report/, [dostęp: 11.04.2025].

[13] A. Ruiz-Gómez, *Commercial Sharenting ...,* op. cit., s. 46.

[14] Ibidem.

[15] A. Kwiatkowska, Z. Kosowska, K. Oleszkiewicz, S. Adamczyk, P. Przemyska, *Era (dez) informacji: praktyczny podręcznik dla kadry nauczycielskiej: edukacja, scenariusze, ćwiczenia*, NASK Państwowy Instytut Badawczy, Warszawa 2024, s. 50.

produkty, nagrody, prowizje oparte na kupujących, korzystających ze spersonalizowanych kodów promocyjnych oraz zaproszenia na wydarzenia lub atrakcje. Współpraca między reklamodawcami a twórcami treści, wynegocjowana poza platformami, nie generuje przychodów platformy.

Commercial sharenting jako sposób na osiągnięcie korzyści

Wraz z upowszechnianiem się zjawiska sharentingu, rośnie liczba rodziców, którzy w otwartym dzieleniu się życiem prywatnym swoich dzieci zauważają sposób na uzyskanie zysku. Dzieci stają się wówczas nie tylko „narzędziem do zwrócenia uwagi na rodzica i pozyskiwania nowych followersów”[16], lecz także „narzędziem do zarabiania pieniędzy bez prawnych instrumentów pozwalających sprzeciwić się działaniom rodziców”[17].

Commercial sharenting można tłumaczyć jako udostępnianie zdjęć, filmów i informacji z życia dziecka, z zamiarem uzyskania korzyści finansowej[18], przy czym korzyścią tą może być natychmiastowe wynagrodzenie, rozwój biznesu, który w przyszłości przyniesie zysk lub inne formy potencjalnego generowania przychodów[19]. Termin ten obejmuje zarówno profesjonalnych twórców treści, influencerów o dużych zasięgach internetowych, którzy zarabiają na tworzeniu treści cyfrowych w ramach przedsięwzięcia biznesowego (jak na przykład influencerzy parentingowi lub influencerzy, którzy stają się rodzicami), jak i coraz częściej zwykłych twórców – rodziców kierowanych chęcią monetyzacji dzieci, którzy mają na celu uzyskanie dodatkowego dochodu[20].

Zjawisko dotyczy najczęściej najmłodszych dzieci – przed ukończeniem 9-10 roku życia. Treści związane z ich życiem stanowią podstawę do

[16] M. Kierzkowska, *Sharenting – pomiędzy prawem rodzica do wyrażania siebie w mediach społecznościowych a ochroną prywatności dziecka*, Kultura i wychowanie, t. 22, nr 2, 2022, s. 50.

[17] *Rodzinka w barterze. Weszliśmy za kulisy biznesu opartego na dzieciach*, https://spidersweb.pl/plus/2023/06/instagram-rodzice-dzieci-barter-wspolpraca-reklama-zarobki, [dostęp: 11.04.2025].

[18] *TikTok Parents Are Taking Advantage of Their Kids. It Needs to Stop*, https://www.cnet.com/tech/services-and-software/tiktok-parents-are-taking-advantage-of-their-kids-it-needs-to-stop/, [dostęp: 08.04.2025].

[19] L. A. Plunkett, *Sharenthood: Why We Should Think Before We Talk about Our Kids Online*, MIT Press, Cambridge 2019, s. 55.

[20] A. Ruiz-Gómez, *Commercial Sharenting ...,* op. cit., s. 147.

budowania kapitału społecznego, który w konsekwencji pozwala na otrzymywanie prezentów, nagród i podpisywanie współpracy z różnymi markami.

W odniesieniu do rodziców, którzy dzielą się własnym doświadczeniem rodzicielskim w celu osiągnięcia korzyści, stosuje się również określenia sharenting labor (praca oparta na sharentingu) i professional sharenting (profesjonalny sharenting). Pierwsze z nich jest tłumaczone jako łączenie praktyk rodzicielskich i pracy influencerów, drugie opiera się na przekształceniu tworzenia treści w karierę zawodową[21]. W tym przypadku rozróżnienie następuje nie ze względu na sposób działalności sharentingowej, lecz przede wszystkim na poziom profesjonalizacji twórcy.

Nieco inny podział opiera się na rodzaju treści, które pozwoliły twórcom na zdobycie uznania w sieci, dzieląc ich na influencerów, którzy zostali rodzicami (osoby, które zdobyły uznanie w sieci na długo przed byciem rodzicami) oraz rodziców, którzy zostali influencerami (osoby, które swoje doświadczenie rodzicielskie wykorzystują jako główny cel swoich treści). W przypadku pierwszej z grup, macierzyństwo/tacierzyństwo włączone do publikowanych treści, może zarówno odgrywać rolę drugorzędną, stanowiąc stały lub tymczasowy rodzaj treści, jak i stać się głównym tematem udostępnianych materiałów. Ta grupa influencerów jest bardzo atrakcyjna dla marketingowców produktów związanych z szeroko pojętym rodzicielstwem – duże zasięgi twórcy stanowią idealną publiczność dla materiałów reklamowych różnych firm. Druga grupa, influencerzy parentingowi (ang. parenting influencers), koncentruje swoje treści wokół ich doświadczeń rodzicielskich, ich dzieci i życia rodzinnego[22].

W poniższej tabeli zaprezentowano najważniejsze aspekty, które różnicują sharenting i commercial sharenting – motywy działania, charakterystykę rodzica oraz potencjalne grono odbiorców treści.

[21] Ibidem, s. 152.

[22] Ibidem, s. 152-155.

Tabela 1. Porównanie sharentingu i commercial sharentingu

Sharenting	Commercial sharenting	
Charakterystyka rodziców		
Zwykli rodzice, którzy dzielą się treściami z rodziną i przyjaciółmi	Blogerzy parentingowi, influencerzy, którzy stali się rodzicami	Rodzice aspirujący na influencerów, rodzice szukający zysku
Charakterystyka aktywności w kontekście sharentingu		
Udostępnianie treści, w celu zaspokojenia potrzeb związanych z komunikacją i kontaktami społecznymi Poszukiwanie informacji dotyczących dzieci – na przykład na rodzicielskich grupach społecznościowych W przypadku wątpliwości odnośnie do prywatności rodzice mogą wdrażać środki mające na celu jej ochronę	Wplatanie w dotychczasową działalność cyfrową treści rodzicielskich Wykorzystywanie zdobytych wcześniej zasięgów do współpracy z firmami zajmującymi się produktami dla dzieci i rodziców W wielu przypadkach tworzenie treści stanowi formę pracy i źródła utrzymania	Stosowanie różnych taktyk, aby zwiększyć zasięg i widoczność Działania mające na celu przyciągnięcie uwagi jak największej liczby odbiorców w celu uzyskania propozycji współpracy Potencjalny zysk może być ważniejszy niż zapewnienie dziecku prywatności
Motywacja dla sharentingu		
Wzmacnianie więzi społecznych: kontakty towarzyskie, wsparcie społeczne, wyrażanie siebie i potrzeba poczucia przynależność. Szukanie informacji o rodzicielstwie, potrzeba wsparcia emocjonalnego	Motywacja napędzana chęcią zysku	
Charakterystyka celowanych odbiorców treści		
Rodzina i przyjaciele Inni rodzice (np. na grupach rodzicielskich)	Wyselekcjonowane grupy odbiorców na podstawie treści udostępnianych przed pojawieniem się dziecka	Inni rodzice Przedstawiciele firm związanych z produktami dla dzieci i rodziców

Źródło: opracowanie własne na podstawie: A. Ruiz-Gómez, *Commercial Sharenting on Instagram: How Parents Build Social Capital and Monetize Baby Accounts Sharenting. Tesis doctoral*, Universidad Complutense De Madrid, Madrid 2023, s. 172.

W każdym z opisanych przypadków rodzicielstwo może otworzyć przed twórcami dodatkowe źródła dochodu przez promowanie określonych, najczęściej powiązanych z tematyką dzieci produktów, jednakże rodzice, którzy dopiero rozpoczynają swoją influencerską działalność, muszą w pierwszej

kolejności przyciągnąć uwagę dużej liczby odbiorców. Wiąże się to najczęściej z upublicznieniem konta i wdrażaniem różnych technik zwiększających jego widoczność.

Zwiększenie liczby obserwatorów wymaga znalezienia sposobu na przyciągnięcie uwagi, niezbędnym jest więc atrakcyjne relacjonowanie życia dziecka. Bardzo często budowanie przyszłej marki rozpoczyna się jeszcze w czasie ciąży – zazwyczaj od publikowania zdjęć ultrasonograficznych płodu lub wręcz od pokazania pozytywnego testu ciążowego. W badaniach przeprowadzonych w 2010 roku wśród rodziców z 10 krajów świata wykazano, że cyfrowy ślad poniżej drugiego roku życia miało 81% dzieci, przy czym średnia dla państw europejskich wyniosła 73%. Za średnią datę cyfrowych narodzin uznano wówczas szósty miesiąc życia dziecka[23].

W serwisach społecznościowych można odnaleźć mnóstwo profili, na których widnieje wizerunek dzieci – co roku dorośli udostępniają w sieci średnio 300 zdjęć swojego dziecka – przeciętni rodzice opublikują więc 1500 zdjęć przed ukończeniem przez nie piątego roku życia[24]. Wiele z tych materiałów to żywe reklamy produktów różnorodnych marek – do niemowląt i kilkulatków można bowiem przypisać treści bardzo szerokiej grupy produktów. To zarówno kosmetyki do pielęgnacji, zabawki i wózki, jak i akcesoria przydatne rodzicom – laktatory, ekspresy do mleka czy nawet meble do pokoju dziecięcego. Skala problemu jest większa niż może się wydawać – niektórzy rodzice przekształcają swoje pociechy w produkty marketingowe restauracji przyjaznych rodzinom, bawialni dla najmłodszych czy wręcz hoteli z ciekawym zapleczem dla dzieci.

Według badania zleconego przez platformę Facebook w 2016 roku osoby, które dopiero co zostały rodzicami, publikują ponad dwa razy więcej zdjęć, prawie trzy razy więcej filmów i prawie dwa razy więcej aktualizacji swojego statusu. Udostępniane przez nich posty dotyczące wiadomości o dziecku otrzymują też więcej interakcji niż pozostałe. Świadczy to o tym, że narodziny dziecka znacznie zwiększają aktywność w mediach społecznościowych[25]. Kidfluencerzy, czyli dzieci, które tworząc treści cyfrowe zdobyły

[23] B. Chrostowska, *Sharenting – skala i wielowymiarowość zjawiska (nierozważnego) ujawniania przez rodziców informacji dzieciach w mediach społecznościowych*, Problemy wczesnej edukacji, t. 43, nr 4, 2018, s. 60.

[24] R. Parenting, *Sharenting: Is It Good or Bad?* https://www.recparenting.com/for-parents/sharenting-should-you-post-photos-of-your-kid-online/, [dostęp: 11.04.2025].

[25] A. Ruiz-Gómez, *Commercial Sharenting on Instagram, op. cit.*, s. 111.

znaczną popularność w mediach społecznościowych, mogą „wygenerować milionowe odsłony w polskim internecie i mają setki tysięcy subskrybentów”[26].

Kidfluencing jako zagrożenie dzieciństwa

Dyskusje, odnośnie do komercyjnych form sharentingu, można podzielić na dwie główne kategorie. Pierwsza z nich skupia się na kwestiach prywatności dziecka i napięciach między prawem małoletnich do prywatności, prawem dorosłych do wyrażania siebie cyfrowo oraz prawem rodzicielskim do podejmowania decyzji odnośnie do aktywności ich dziecka w Internecie. Druga grupa koncentruje się z kolei na uznaniu aktywności dziecka jako pracy w charakterze twórcy cyfrowego.

Do skrzynek odbiorczych profili różnorodnych marek trafiają każdego dnia wiadomości z propozycją współpracy. Coraz częściej są to pytania od młodych mam, które marząc o karierze influencerki w zamian za produkt oferują post z reklamą marki na swoim koncie. „Prowadzę profil na Insta, mogę zrobić zdjęcie, tekst, unboxing, pokazać produkt. Czy są Państwo zainteresowani współpracą barterową?”[27] – to pytania, które stały się dla marketerów codziennością. Influencerzy o największych zasięgach potrafią nawet nie pytać – publikują na swoich kontach informację, że czegoś potrzebują, lub proszą o poradę odnośnie do wyboru jakiegoś produktu i liczą na bezpośredni odzew od firm z propozycją współpracy[28].

Dzieci-manekiny, słupy reklamowe – to określenia, które coraz częściej pojawiają się w kontekście kilkulatków na profilach społecznościowych[29]. Niczego nieświadome małe dzieci – zarówno te kilkuletnie, jak i kilkumiesięczne – prezentują modne ubrania, kosmetyki i jedzenie dla niemowląt, drogie zabawki i inne produkty związane z szeroko pojętym rodzicielstwem.

---

[26] *Dziecięcy influencerzy mają zarobki i zasięgi, o jakich marzy wielu. Tylko jakim kosztem...*, https://android.com.pl/tech/802007-sharenting-kid-influencer-dzieci-siec/, [dostęp: 12.04.2025].

[27] *Rodzinka w barterze. Weszliśmy za kulisy biznesu opartego na dzieciach*, https://spidersweb.pl/plus/2023/06/instagram-rodzice-dzieci-barter-wspolpraca-reklama-zarobki, [dostęp: 11.04.2025].

[28] Ibidem.

[29] *Kidfluencerzy i dzieci manekiny. Jak instarodzice zamieniają dzieciństwo w towar*, https://spidersweb.pl/plus/2023/04/kidfluencerzy-dziecinstwo-rodzice-instagram, [dostęp: 11.04.2025].

Kwestią, nad którą również należałoby się zastanowić w przypadku zarabiania na wizerunku dzieci w Internecie, jest wprowadzanie odbiorców w błąd. Z uwagi na to, że rodzice prowadzący działalność komercyjną proszą swoje dzieci o przekazywanie informacji w określony sposób, konsumenci mogą myśleć, że posty są autentyczne, mogą również otrzymywać zniekształcone poglądy na temat produktów[30]. Ciężko jest natomiast mówić o swoich doświadczeniach z produktem, który nie został wcześniej wypróbowany, a przecież dzieci mogą nie mieć wystarczającego doświadczenia, aby móc go rzetelnie promować[31].

Obecnie polskie prawo nie reguluje wprost sposobów na oznaczanie materiałów reklamowych w mediach społecznościowych, jednak konsumenci powinni być poinformowani, jeśli przekaz ma charakter nie neutralny, lecz handlowy. Zgodnie z zaleceniami Prezesa Urzędu Ochrony Konkurencji i Konsumentów materiały reklamowe powinny być wyraźnie odróżnione i oznaczane w sposób, który na żadnym z etapów zapoznawania się z nimi nie budzi wątpliwości – „czytelny, jednoznaczny oraz zrozumiały dla każdego odbiorcy”[32].

Niektórzy uznają, że gdy dzieci tylko występują na fotografii, to nie pracują, inni postrzegają działalność marketingową na dzieciach jako „stwarzanie możliwości dawania dzieciom rzeczy, na które inaczej nie mogliby sobie pozwolić”[33]. Niemniej jednak commercial sharenting jest czerpaniem zysków z wizerunku dziecka w Internecie – rodzice zawierają umowy i wyrażają świadomą zgodę, aby ich dziecko było przedstawione w określony sposób – najczęściej bez uprzedniego pytania o jego zdanie lub/i zgodę. Aby dopełnić zobowiązań sponsorskich nierzadko muszą przygotować odpowiednią liczbę postów, do tego dochodzą treści, które choć nie są wynikiem współpracy, są istotne dla zapewnienia obserwujących, że dany profil nie jest wyłącznie reklamą. Problem pojawia się, gdy danego dnia dziecko nie jest zainteresowane tworzeniem nowego materiału i nie chce uczestniczyć w procesie jego przygotowania. Wówczas niektórzy rodzice przekupują przyszłego aktora

[30] M. N. Fineman, *Honey, I Monetized the Kids: Commercial Sharenting and Protecting the Rights of Consumers and the Internet's Child Stars*, *op. cit.*, s. 873.

[31] Ibidem, s. 873-874.

[32] *Rekomendacje Prezesa UOKiK dotyczące oznaczania treści reklamowych przez influencerów w mediach społecznościowych*, Warszawa 2022, s. 16.

[33] M. N. Fineman, *Honey, I Monetized the Kids: Commercial Sharenting …*, op. cit., s. 869.

reklamy – „Chyba, że jest to praca zarobkowa (...). Wtedy muszą tam być. W te dni zawsze mamy lizaki”[34].

Mimo, że niektórzy odkładają przynajmniej część wynagrodzenia na przyszłość dziecka, pozostali traktują je jako własny zarobek. W pewnym sensie dochody dorosłych stają się zależne od dzieci – mimo, że to dorośli kształtują końcową wersję udostępnianych treści, wielokrotnie kluczem do ich sukcesu są właśnie małoletni. Co więcej, nierzadko na dzieciach wywierana jest presja utrzymywania rodziny.

Mówiąc o działalności opartej na monetyzacji dzieci można stwierdzić, że „rodzice stają się pracodawcami, a ich dzieci stają się prawnie niechronionymi, niechętnymi pracownikami, zmuszonymi do odgrywania swojego dzieciństwa zamiast faktycznie je przeżywać”[35]. Leah Plunkett z Harvard Law twierdzi, że rodzice „zmuszają dzieci do zachowywania się tak, jakby były sobą, zamiast dawać im prywatność do zabawy – tak, aby mogły odkryć kim naprawdę są”[36]. W przeciwieństwie do dzieci w tradycyjnych reklamach, gdzie młodzi aktorzy przyjmują rolę innej osoby, w przypadku commercial sharentingu dzieci grają samych siebie.

Rozwiązania prawne

Praca polegająca na byciu influencerem, w szczególności praca dziecka w takim charakterze, nie jest uregulowana przez polski system prawny, jednakże rosnący udział dzieci w sektorze rozrywki w mediach społecznościowych podkreśla potrzebę regulacji tej kwestii.

W Stanach Zjednoczonych pewne aspekty są regulowane ustanowionym w 1939 roku prawem Coogana (zwanym również jako California Child Actor’s Bill). Początkowo dotyczyło ono dzieci-aktorów przemysłu filmowego, z czasem rozszerzając swój zakres do branży telewizyjnej, i miało chronić najmłodszych przez ustalenie zasad godzin pracy i odpoczynku oraz przez zabezpieczenie części ich zarobków. Rodzice zostali zobowiązani do odkładania 15% wynagrodzenia na specjalnie do tego celu utworzonym funduszu powierniczym, który jest nienaruszalny aż do osiągnięcia przez małoletniego

[34] Ibidem, s. 882.

[35] *Their Parents Were Family Influencers, Now Their Kids Hate Them*, https://futurism.com/parents-influencers-kids-hate-them, [dostęp: 12.04.2025].

[36] M. N. Fineman, *Honey, I Monetized the Kids: Commercial Sharenting and Protecting the Rights of Consumers and the Internet’s Child Stars*, *op. cit.*, s. 867.

pełnoletności. Prawo to nie obejmuje jednak dzieci, które zarabiają za pośrednictwem mediów społecznościowych[37].

W lipcu 2024 roku w Stanach Zjednoczonych przyjęto ustawę o bezpieczeństwie dzieci w Internecie (ang. Kids Online Safety and Privacy Act – KOSPA)[38]. Jest pakietem legislacyjnym obejmującym dwa projekty ustaw i zawierającym przepisy, które[39]:

- wymagają od firm zarządzających mediami społecznościowymi, aby projektowały swoje platformy w sposób, w którym bezpieczeństwo i prywatność dzieci i młodzieży będą priorytetem bardziej istotnym niż zysk;
- dają małoletnim i ich rodzicom większą kontrolę nad korzystaniem z mediów społecznościowych oraz narzędzia do zgłaszania szkód wyrządzonych na objętych ochroną platformach;
- minimalizują ilość danych gromadzonych od małoletnich i wymagają zgody nastolatków, lub w przypadku dzieci poniżej 13 roku życia rodziców, na zbieranie tych danych;
- zakazują kierowania spersonalizowanych reklam do małoletnich.

Wszystkie powyższe zalecenia firmy muszą wprowadzić w sposób, który jednocześnie umożliwia dzieciom dostęp online do społeczności, edukacji i rozrywki.

KOSPA co prawda zwiększa presję na platformy, by nie wspierały szkodliwych praktyk i zapewniały lepszą ochronę dzieciom, ale nie rozwiązuje bezpośrednio problemu wykorzystywania dzieci przez rodziców w celach zarobkowych.

Na problem braku regulacji chroniących dzieci biorących udział w tworzeniu treści cyfrowych zwróciła uwagę również Izba Gmin Wielkiej Brytanii w opublikowanym przez siebie w maju 2022 roku raporcie „Influencer culture: Lights, camera, inaction?". Zwrócono w nim uwagę, że „agencje influencerów postrzegają rodzinnych influencerów jako jedne z najbardziej pożądanych

[37] Ibidem, s. 880.

[38] *Contextualizing the Kids Online Safety and Privacy Act: A Deep Dive into the Federal Kids Bill*, https://fpf.org/blog/contextualizing-the-kids-online-safety-and-privacy-act-a-deep-dive-into-the-federal-kids-bill/, [dostęp: 12.04.2025].

[39] *KOSPA One Pager 2024 - Common Sense Media*, https://www.commonsensemedia.org/sites/default/files/featured-content/files/kospa-one-pager-2024-updated-12.10.24.pdf, [dostęp: 12.04.2025].

gwiazd mediów społecznościowych […], ponieważ są atrakcyjni zarówno dla dzieci, jak i rodziców”[40].

Zgodnie z dokumentem istnieją trzy istotne kwestie do dyskusji[41]:

- prawo do prywatności dzieci w mediach społecznościowych;
- kwestia wynagrodzenia dzieci za ich cyfrową pracę;
- uregulowanie godzin i warunków pracy – tak, aby nie miała ona negatywnego wpływu na doświadczenia dzieci.

Jednym z krajów, w którym cyfrowa praca małoletnich jest regulowana przepisami, jest Francja, która pod koniec 2020 roku uchwaliła prawo chroniące dzieci-influencerów poniżej 16 roku życia. Z jego zapisów wynika przede wszystkim regulacja godzin pracy oraz zabezpieczenie dochodów uzyskanych z pracy w mediach społecznościowych na specjalnie do tego celu utworzonych kontach[42]. Co więcej, w określonych przypadkach na produkcję filmów komercyjnych rodzice i firmy muszą uzyskać pozwolenie od władz. Poza wyznaczonym progiem wiekowym praca kidfluencerów jest pozostawiona do decyzji rodziców.

Prawo francuskie pozwala też dzieciom żądać, aby platformy usuwały filmy z ich wizerunkiem bez konieczności uzyskania zgody rodziców. Należy jednak pamiętać, że wiele dzieci bierze udział w tworzeniu treści już od najmłodszych lat – nie są więc oni w stanie zgodzić się na rozpowszechnianie ich wizerunku ani zażądać usunięcia takich treści[43].

Przepisy prawa obowiązujące w Polsce nie regulują zjawiska sharentingu wprost, a zapisy odnoszące się do ochrony prywatności i wizerunku dziecka są rozproszone w kilku aktach prawnych[44]. Jednym z nich, mającym na celu zapewnienie dzieciom właściwej ochrony i prawa do prawidłowego rozwoju, jest ratyfikowana przez Polskę w 1991 roku Konwencja o prawach dziecka. Ustanawia ona szereg praw dzieci – cywilnych, socjalnych,

[40] *Social media: Rise of ‘kidfluencers’ pushes legislators to engage with children’s rights online*, https://www.ibanet.org/Social-media-Rise-of-kidfluencers-pushes-legislators-to-engage-with-childrens-rights-online, [dostęp: 09.04.2025].

[41] Ibidem.

[42] A. Ruiz-Gómez, *Commercial Sharenting o…,* op. cit., s. 170.

[43] *Social media: Rise of ‘kidfluencers’ pushes legislators to engage with children’s rights online*, https://www.ibanet.org/Social-media-Rise-of-kidfluencers-pushes-legislators-to-engage-with-childrens-rights-online, [dostęp: 09.04.2025].

[44] J. Maniszewska-Ejsmont, *Sharenting a prawa dziecka – rozważania nad władzą rodzicielską w dobie mediów społecznościowych*, Palestra – Pismo Adwokatury Polskiej, nr 4, 2022, s. 78.

kulturowych i politycznych, chroniąc wszystkich ludzi poniżej 18 roku życia na zasadach niedyskryminacyjnych[45].

W kontekście sharentingu należy z jej zapisów wymienić przede wszystkim[46]:

- artykuł 16, zgodnie z którym dziecko nie może być poddawane arbitralnej lub bezprawnej ingerencji w jego prywatność, rodzinę, dom lub korespondencję, ani być ofiarą bezprawnych zamachów na jego honor i reputację;
- artykuł 3, który nakłada na państwa-strony obowiązek działania na rzecz zapewnienia dziecku ochrony prawnej przed taką ingerencją lub atakami.

Prawa i obowiązki dziecka określono również w Konstytucji Rzeczypospolitej Polskiej, zgodnie z którą źródłem wolności i praw człowieka jest przyrodzona i niezbywalna, nienaruszalna godność. Dokument mówi też o fundamentalnym prawie do ochrony życia prywatnego oraz do decydowania o swoim życiu osobistym[47].

Konstytucja określa również prawa rodziców, stanowiąc, że mogą oni wychowywać dzieci zgodnie z własnymi przekonaniami (przy uwzględnieniu stopnia dojrzałości dziecka, jego wolności sumienia i przekonania)[48]. Prawo konstytucyjne precyzuje Kodeks rodzinny i opiekuńczy, zgodnie z którym rodzice są zobowiązani do wychowywania dziecka z poszanowaniem jego godności i praw i z dbałością o jego dobro i interes społeczny, a przed podjęciem decyzji istotnie wpływających na dziecko, do wysłuchania go i w miarę możliwości do uwzględnienia jego rozsądnych życzeń[49].

Rozważając o konsekwencjach sharentingu nie sposób nie poruszyć tematu prywatności dziecka i przysługującego mu, jak i każdej osobie dorosłej, prawie do ochrony wizerunku[50]. Wizerunek jest nie tylko dobrem osobistym, lecz także jednym z podstawowych praw opisanych w Europejskiej Konwencji

[45] Konwencja o prawach dziecka, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 r. *(Dz. U. 1991 Nr 120, poz. 526), art. 1-2.*

[46] Ibidem, art. 3, 16.

[47] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 Nr 78, poz. 483), art. 30, 47.

[48] Ibidem, art. 48.

[49] Ustawa z dnia 25 lutego 1964 r. - Kodeks rodzinny i opiekuńczy (Dz. U. 1964 Nr 9, poz. 59), art. 92, 95.

[50] Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. 1964 Nr 16, poz. 93), art. 23.

Praw Człowieka[51]. Wizerunek jest też chroniony przepisami Ustawy o prawie autorskim i prawach pokrewnych oraz Ustawy o ochronie danych osobowych.

Rozpowszechnianie wizerunku danej osoby (bez względu na jej wiek) wymaga co do zasady jej zgody[52]. W przypadku dzieci, które nie mają pełnej zdolności do czynności prawnych, do osiągnięcia pełnoletniości, zgody tej udzielają ich przedstawiciele ustawowi – rodzice lub opiekunowie prawni. Obecnie o zgodę na publikację zdjęcia pyta dziecko jedynie co czwarty rodzic[53], jednak niewątpliwie od niemowlęcia lub kilkuletniego dziecka ciężko jest taką zgodę w ogóle uzyskać.

Wizerunek to również jedna z danych osobowych, czyli „informacji o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej"[54]. Jego przetwarzanie (a więc i rozpowszechnianie w sieci), podlega ochronie przepisami ogólnego rozporządzenia o ochronie danych[55]. Zgodnie z dokumentem dane osobowe osób małoletnich podlegają szczególnej ochronie, ponieważ dzieci mogą nie być świadome ryzyka, konsekwencji, zabezpieczeń i przysługujących im praw[56].

Unijne rozporządzenie formułuje również prawo do bycia zapomnianym[57]. Prawo to pozwala osobom fizycznym, których dane osobowe dotyczą, żądania od dostawców usług internetowych usunięcia tych danych. Jednakże małoletni, których dane zostały udostępnione przez rodziców, przed osiągnięciem pełnoletności nie są uprawnieni do skorzystania ze swojego prawa. Należy się również zastanowić, czy w erze cyfrowej komunikacji i dzieciństwa

[51] Konwencja o ochronie praw człowieka i podstawowych wartości sporządzona w Rzymie dnia 4.11.1950 r. (Dz. U. 1993 r. Nr 61, poz. 284 ze zm.).

[52] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. 1994 Nr 24, poz. 83), art. 81.

[53] A. Kwaśnik, Z. Polak, P. Sowiński, *Cyfrowy ślad małego dziecka*, NASK - Państwowy Instytut Badawczy, Warszawa 2021, s. 7.

[54] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L L 119/1), art. 4.

[55] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

[56] Ibidem, motyw 38.

[57] Ibidem, art. 17.

opartego na danych, istnieje jakakolwiek gwarancja, że platformy i sieci komercyjne, kiedykolwiek zapomną o czymkolwiek[58].

W literaturze przedmiotu można się spotkać z dyskusją odnośnie do stopnia, w jakim prawa dziecka do prywatności stoją w konflikcie z prawem dorosłych do wolności wypowiedzi, jednakże niepodważalna w międzynarodowym porządku prawnym zasada kierowania się dobrem dziecka wymaga, aby w sytuacjach kolidowania interesów dziecka i rodzica stawiać na pierwszym miejscu najlepszy interes małoletniego[59].

Ostatecznie, zgodnie z Kodeksem pracy dziecko, które nie ukończyło 16 roku życia, może podjąć pracę lub zajęcie zarobkowe wyłącznie na rzecz działalności kulturalnej, artystycznej, sportowej lub reklamowej, jednak wyłącznie za zgodą opiekuna prawnego i inspektora pracy[60]. Praca ta nie może stanowić zagrożenia życia, zdrowia, rozwoju psychofizycznego dziecka oraz wypełniania przez niego obowiązku szkolnego. O braku przeciwskazań mają twierdzić wymagane w załącznikach do wniosku orzeczenia i opinie (w tym opinię poradni psychologiczno-pedagogicznej, orzeczenie lekarza i jeżeli dziecko podlega obowiązkowi szkolnemu, opinię dyrektora szkoły)[61]. Retorycznym wydaje się być pytanie, czy kilkuletnie dziecko jest w stanie taką zgodę uzyskać.

Podsumowanie

Zjawisko commercial sharentingu wpisuje się w szeroki kontekst zagrożeń związanych z cyfryzacją życia społecznego. Pokazuje jak silnie media społecznościowe zredefiniowały dzieciństwo, rodzicielstwo i pracę.

Wykorzystywanie wizerunku dziecka jako narzędzia służącego osiąganiu korzyści finansowych, materialnych czy wizerunkowych niesie ze sobą dotkliwe konsekwencje dla bezpieczeństwa psychicznego, emocjonalnego

[58] T. Leaver, *Balancing Privacy: Sharenting, Intimate Surveillance and the Right to Be Forgotten,* [w:] *The Routledge Companion to Digital Media and Children*, L. Green, D. Holloway, K. Stevenson, T. Leaver, L. Haddon (red.), Routledge, New York 2020, s. 240.

[59] *Sharenting a prawa dziecka – rozważania nad władzą rodzicielską w dobie mediów społecznościowych*, https://palestra.pl/pl/czasopismo/wydanie/4-2022/artykul/sharenting-a-prawa-dziecka-rozwazania-nad-wladza-rodzicielska-w-dobie-mediow-spolecznosciowych, [dostęp: 10.04.2025].

[60] N. Kurtieva, *Kiedy można zatrudnić osobę poniżej 18. roku życia*, https://biznes.gov.pl/pl/portal, [dostęp: 11.04.2025].

[61] Ibidem.

oraz tożsamościowego małoletniego. Dziecko, bez świadomości skutków swojej obecności w sieci, zostaje włączone w procesy marketingowe – często bez właściwej ochrony prawnej i bez realnego wpływu na podejmowane za nie decyzje.

Z praktyką commercial sharentingu wiąże się szereg zagrożeń fundamentalnych praw dziecka. Aktualnie w polskich przepisach nie istnieją odrębne zapisy, które regulowałyby to zjawisko. Choć w niektórych dokumentach można znaleźć pewne formy ochrony dla wizerunku i danych osobowych dziecka lub też nakazy kierowania się w wychowaniu dziecka jego najlepszym interesem, w wielu przypadkach są to przepisy martwe, bowiem przed osiągnięciem pełnoletności to rodzice podejmują wszelkie decyzje w imieniu małoletnich. Jeśli więc stwierdzą oni, „że relacjonowanie jego życia, nawet od pierwszych dni, i zarabianie na wizerunku dziecka jest w porządku, to nikt nie ma mocy prawnej, aby coś z tym zrobić”[62].

Poza niewątpliwie poważnymi konsekwencjami naruszeń prywatności dzieci, należy również wziąć pod uwagę inny aspekt, jakim jest przedmiotowe traktowanie dzieci. Małoletni wciąż zbyt rzadko mają realny wpływ na decyzje dotyczące spraw, które ich bezpośrednio dotyczą. Tymczasem istotną część ich prawa do prywatności i do kształtowania własnej tożsamości – zarówno w przestrzeni cyfrowej, jak i rzeczywistej – stanowi możliwość decydowania o udostępnianiu własnego wizerunku w Internecie.

Zjawisko commercial sharentingu stawia poważne pytania o granice prywatności, godność dziecka i odpowiedzialność dorosłych – nie tylko rodziców, lecz także marek, platform i ustawodawców. Wobec jego rosnącej skali konieczne staje się wypracowanie skutecznych narzędzi prawnych i etycznych. Podejście uwzględniające zarówno wymiar technologiczny, społeczny, jak i prawny sharentingu może zagwarantować realną ochronę najmłodszych w dynamicznie zmieniającym się środowisku cyfrowym – środowisku, o którego istnieniu często nawet jeszcze nie wiedzą.

Literatura

1. Kwaśnik A., Polak Z., Sowiński P., *Cyfrowy ślad małego dziecka*, NASK - Państwowy Instytut Badawczy, Warszawa 2021.

[62] *Kidfluencerzy, rodzice i dzieci w social mediach*, https://spidersweb.pl/plus/2023/04/kidfluencerzy-dziecinstwo-rodzice-instagram, [dostęp: 23.03.2025].

2. Kwiatkowska A., Kosowska Z., Oleszkiewicz K., Adamczyk S., Przemyska P., *Era (dez)informacji: praktyczny podręcznik dla kadry nauczycielskiej: edukacja, scenariusze, ćwiczenia*, NASK Państwowy Instytut Badawczy, Warszawa 2024.
3. Plunkett L.A., *Sharenthood: Why We Should Think Before We Talk about Our Kids Online*, MIT Press, Cambridge 2019.
4. Ruiz-Gómez A., *Commercial Sharenting on Instagram: How Parents Build Social Capital and Monetize Baby Accounts Sharenting. Tesis doctoral*, Universidad Complutense De Madrid, Madrid 2023.
5. Brosch A., *Sharenting – Why Do Parents Violate Their Children's Privacy?*, The New Educational Review, t. 54, 2018.
6. Chrostowska B., *Sharenting – skala i wielowymiarowość zjawiska (nierozważnego) ujawniania przez rodziców informacji dzieciach w mediach społecznościowych*, Problemy Wczesnej Edukacji, t. 43, nr 4, 2018.
7. Fineman M.N., *Honey, I Monetized the Kids: Commercial Sharenting and Protecting the Rights of Consumers and the Internet's Child Stars*, The Georgetown Law Journal, t. 11, nr 4, 2023.
8. Kierzkowska M., *Sharenting – pomiędzy prawem rodzica do wyrażania siebie w mediach społecznościowych a ochroną prywatności dziecka*, Kultura i wychowanie, t. 22, nr 2, 2022.
9. Maniszewska-Ejsmont J., *Sharenting a prawa dziecka – rozważania nad władzą rodzicielską w dobie mediów społecznościowych*, Palestra – Pismo Adwokatury Polskiej, nr 4, 2022.
10. Yates C., *Influencing „Kidfluencing": Protecting Children by Limiting the Right to Profit From „Sharenting"*, Vanderbilt Journal of Entertainment & Technology Law, t. 25, nr 4, 2023.
11. Leaver T., *Balancing Privacy: Sharenting, Intimate Surveillance and the Right to Be Forgotten*, [w:] *The Routledge Companion to Digital Media and Children*, L. Green, D. Holloway, K. Stevenson, T. Leaver, L. Haddon (red.), Routledge, New York 2020.
12. *Rekomendacje Prezesa UOKiK dotyczące oznaczania treści reklamowych przez influencerów w mediach społecznościowych*, Warszawa 2022.

Akty prawne

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 Nr 78, poz. 483).
2. Konwencja o ochronie praw człowieka i podstawowych wartości sporządzona w Rzymie dnia 4.11.1950 r. (Dz. U. 1993 Nr 61, poz. 284 ze zm.).
3. Konwencja o prawach dziecka, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 r. (Dz. U. 1991 Nr 120, poz. 526).
4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L L 119/1).

5. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. 1994 Nr 24, poz. 83).
6. Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny Dz. U. 1964 Nr 16, poz. 93).
7. Ustawa z dnia 25 lutego 1964 r. - Kodeks rodzinny i opiekuńczy (Dz. U. 1964 Nr 9, poz. 59).

Netografia

1. *Contextualizing the Kids Online Safety and Privacy Act: A Deep Dive into the Federal Kids Bill*, https://fpf.org/blog/contextualizing-the-kids-online-safety-and-privacy-act-a-deep-dive-into-the-federal-kids-bill/.
2. *Dziecięcy influencerzy mają zarobki i zasięgi, o jakich marzy wielu. Tylko jakim kosztem...*, https://android.com.pl/tech/802007-sharenting-kid-influencer-dzieci-siec/.
3. *Hub I.M., Influencer Marketing Benchmark Report 2025*, https://influencermarketinghub.com/influencer-marketing-benchmark-report/.
4. *Kidfluencerzy i dzieci manekiny. Jak instarodzice zamieniają dzieciństwo w towar*, https://spidersweb.pl/plus/2023/04/kidfluencerzy-dziecinstwo-rodzice-instagram.
5. *Kidfluencerzy, rodzice i dzieci w social mediach*, https://spidersweb.pl/plus/2023/04/kidfluencerzy-dziecinstwo-rodzice-instagram.
6. *KOSPA One Pager 2024 - Common Sense Media*, https://www.commonsensemedia.org/sites/default/files/featured-content/files/kospa-one-pager-2024-updated-12.10.24.pdf.
7. Kurtieva N., *Kiedy można zatrudnić osobę poniżej 18. roku życia*, https://biznes.gov.pl/pl/portal.
8. Parenting R., *Sharenting: Is It Good or Bad?*, https://www.recparenting.com/for-parents/sharenting-should-you-post-photos-of-your-kid-online/.
9. *Rodzinka w barterze. Weszliśmy za kulisy biznesu opartego na dzieciach*, https://spidersweb.pl/plus/2023/06/instagram-rodzice-dzieci-barter-wspolpraca-reklama-zarobki.
10. *Sharenting a prawa dziecka – rozważania nad władzą rodzicielską w dobie mediów społecznościowych*, https://palestra.pl/pl/czasopismo/wydanie/4-2022/artykul/sharenting-a-prawa-dziecka-rozwazania-nad-wladza-rodzicielska-w-dobie-mediow-spolecznosciowych.
11. *SHARENTING definition and meaning | Collins English Dictionary*, https://www.collinsdictionary.com/dictionary/english/sharenting.
12. *Social media: Rise of 'kidfluencers' pushes legislators to engage with children's rights online*, https://www.ibanet.org/Social-media-Rise-of-kidfluencers-pushes-legislators-to-engage-with-childrens-rights-online.
13. *Their Parents Were Family Influencers, Now Their Kids Hate Them*, https://futurism.com/parents-influencers-kids-hate-them.
14. *TikTok Parents Are Taking Advantage of Their Kids. It Needs to Stop*, https://www.cnet.com/tech/services-and-software/tiktok-parents-are-taking-advantage-of-their-kids-it-needs-to-stop/.

mgr Magdalena Miczek
Wyższa Szkoła Bezpieczeństwa w Poznaniu
ORCID: 0009-0007-5446-4328
https://doi.org/10.29316/9788368103199_18

KSZTAŁTOWANIE POSTAW JAKO JEDEN Z FILARÓW BEZPIECZEŃSTWA PAŃSTWA

FORMATION OF ATTITUDES AS ONE OF THE PILLARS OF STATE SECURITY

Streszczenie

Celem niniejszego rozdziału jest identyfikacja znaczenia kształtowania postaw oraz podkreślenie ich wagi, jako jednego z filarów bezpieczeństwa państwa, a wręcz warunku sine qua non tegoż bezpieczeństwa. Autorka podjęła próbę udowodnienia, że właściwe rozumienie pojęć takich jak: ojczyzna, patriotyzm, naród, poczucie narodowe, dobro wspólne, przekłada się na konkretne postawy jednostki i całego społeczeństwa. Postawy te wzmacniają lub osłabiają bezpieczeństwo państwa, rozumiane jako przetrwanie, integralność, rozwój. W pierwszej części rozdziału zostały przedstawione wybrane pojęcia, ważne z punktu widzenia bezpieczeństwa państwa, analiza i porównanie ich definicji z uwzględnieniem różnic między nimi. Następnie przedstawiono, jak ich rozumienie może wpływać na postawę człowieka. Na zakończenie podkreślono istotę kształtowania postaw, jak również znaczenie tego procesu dla bezpieczeństwa państwa. W pracy wykorzystano następujące metody

Summary

The goal of this chapter is to emphasize the influence of the formation of attitudes as one of the pillars of state security. The author takes an attempt to prove that the correct comprehension of notions such as: homeland, patriotism, nation, national identity, commom good can strengthen or weaken the security of the state understood as survival, integrity and development. The first part of this chapter consist of the analysis of some notions, their definitions and the differences beetwen them. Then it is presented how comprehension of some notions can influence someone's attitude in the context of state security. In the last part the author indicates how crucial are the presented attitudes in terms of building state security. The following research methods and technques were used: subject literatury analysis, legal texts analysis, induction.

i techniki badawcze: analiza literatury przedmiotu, aktów prawnych, indukcja.

Słowa klucze: bezpieczeństwo, bezpieczeństwo państwa, ojczyzna, naród, patriotyzm, poczucie narodowe, dobro wspólne, wspólnota, tożsamość, postawa, kształtowanie postaw, edukacja

Keywords: security, state security, homeland, nation, patriotism, national identity, common good, community, identity, attitude, attitude forming, education

Wstęp

Obowiązkiem obywatela polskiego jest wierność Rzeczypospolitej Polskiej oraz troska o dobro wspólne[1]. Obowiązkiem obywatela polskiego jest obrona Ojczyzny[2]. Oba, wyrażające jasno sformułowaną treść, zdania ustawy zasadniczej, która stanowi najwyższe źródło prawa w Polsce, wydają się oczywistością *per se* i nie budzącym wątpliwości ani zastrzeżeń faktem. Niemniej jednak, biorąc pod uwagę zmiany, jakie miały miejsce od czasu formułowania i uchwalenia Konstytucji RP, a także ich dynamikę, w szczególności rozwój technologii informacyjno-komunikacyjnych, które na niespotkaną do tej pory skalę przyczyniły się do transformacji społeczeństwa z industrialnego, czy już postindustrialnego w informacyjne, zawarte w przytoczonych artykułach zapisy mogą dla współczesnego, szczególnie młodego, człowieka brzmieć górnolotnie i bez pokrycia. Przyczyną takiego stanu rzeczy wydaje się być z jednej strony relatywizacja pojęć, odejście od ich znaczenia w ujęciu klasycznym[3], a także brak poczucia realnych zagrożeń bezpieczeństwa państwa w ostatnich trzech dekadach.

Wybrane pojęcia i ich definicje

Punktem wyjścia do dalszych rozważań jest usystematyzowanie pojęć. Zdefiniowanie właściwego znaczenia i zasadniczego sensu słów ma bowiem kluczowe znaczenie dla ich prawidłowego pojmowania, a przez to

[1] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Dz. U. 1997 Nr 78, poz. 483), art. 82.

[2] Ibidem, art. 85.

[3] Mówiąc o ujęciu klasycznym autor ma na myśli rozumienie pojęć w dorobku cywilizacji łacińskiej opartej na triadzie: filozofia grecka, prawo rzymskie, etyka chrześcijańska.

podejmowania dobrych decyzji oraz skutecznych przedsięwzięć oddziałujących i przekładających się na bezpieczeństwo państwa.

W tym kontekście, kształtowanie właściwych postaw[4] nakierowane na przebicie się do świadomości, nie tylko na poziomie poznawczym, ale przede wszystkim głębokiego zrozumienia i wewnętrznej asymilacji, pojęć takich jak: państwo, ojczyzna, patriotyzm, poczucie narodowe, naród, społeczeństwo, dobro indywidualne, dobro wspólne, jak również zasadniczych różnic między nimi, jest zadaniem ważnym, a wręcz niezbędnym.

Najbardziej podstawową definicję państwa, które jest terminem wieloznacznym, podaje Słownik języka polskiego PWN, jako zorganizowaną politycznie społeczność zamieszkującą określone terytorium, mającą swój rząd i swoje prawa[5]. Wywodzące się od gr. *polis* – gmina pełnoprawnych obywateli i łac. *civitas* -państwo obywateli rzymskich, państwo jest to polityczna organizacja społeczeństwa, funkcjonująca na określonym terytorium i ustanawiająca suwerenne prawo, sprawująca władzę poprzez system trwałych instytucji, finansowanych ze środków publicznych, odpowiadających za całość i cele zbiorowej organizacji życia społecznego[6]. Ta wyposażona w organy władzy organizacja społeczna podlega normom i zasadom tworzącym ład wewnętrzny, które to normy i zasady wyznaczają również członkom tej organizacji określone obowiązki i uprawnienia[7].

Ojczyznę najprościej można zdefiniować jako „kraj, w którym ktoś się urodził i który jest krajem jego rodaków”[8]. Bardziej rozbudowana definicja dodaje elementy, do których należą: uważanie tego kraju za własny, zamieszkiwanie w nim przez dłuższy czas, uczuciowa więź z racji pochodzenia, związków rodzinnych, przywiązanie do określonych wartości, które ten kraj uosabia[9]. ” Ojczyzna, to zwarty obszar, stanowiący stałą bez przerwy siedzibę

[4] Pod pojęciem właściwych postaw, w rozumieniu autora, zawiera się stosunek i postepowanie oparte na normach moralnych oraz cnotach, które przyczyniają się do wzmocnienia i utrzymania bezpieczeństwa państwa, zarówno w obszarze wewnętrznym, jak i zewnętrznym, materialnym i duchowym.

[5] sjp.pwn.pl/szukaj/państwo.html, państwo II, [dostęp: 19.03.2025].

[6] K. Chałas, A. Maj (red.), *Encyklopedia aksjologii pedagogicznej*, Polskie Wydawnictwo Encyklopedyczne, Radom 2016, s. 708.

[7] W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie Uwarunkowania System*, Akademia Obrony Narodowej, Warszawa 2011, s. 22.

[8] *Mały słownik języka polskiego*, Państwowe Wydawnictwo Naukowe, Warszawa 1969, s. 502.

[9] *Wielka Encyklopedia PWN*, Wydawnictwo Naukowe PWN, Warszawa 2002-2005, t. 19, s. 399.

i widownię dziejów narodowych; język ojczysty może być tylko jeden, ten sam od samego początku i bez przerw uprawiany”[10]. To „miejsce lub kraj urodzenia, wychowania i formacji osobowościowej człowieka, zamieszkały przez naród lub narody, któremu zawdzięcza on kulturę materialną i umysłowo – duchową i z którym jest emocjonalnie powiązany przez tradycję i historię”[11]. Pojęcie ojczyzny obejmuje zatem elementy: materialny, antropologiczny, aksjologiczno – kulturowy oraz historyczno – tradycyjny[12], przez co wydaje się pojęciem szerszym, pełniejszym od pojęcia państwa; pojęciem, które może stanowić wartość, przedmiot godny troski, wierności i poświęceń, nadawać sens ludzkiej egzystencji oraz poczucie przynależności, ponieważ „nie można mieć ojczyzny wszędzie i gdziekolwiek, ani też mieć za ojczysty jakiegoś języka sztucznego, uniwersalnego”[13]. Słowo ojczyzna wywodzi się zarówno z greki (gr. *patriótes* rodak, od: *pátrios* pochodzący od tego samego ojca), jak i łaciny (łac. *patria*, od: *pater* ojciec)[14].

Etymologia słowa ojczyzna prowadzi zatem w sposób naturalny do pojęcia patriotyzmu, (gr. *patriótes* rodak, łac. *patria* ojczyzna) rozumianego i postrzeganego jako „cnota moralna powiązana ze sprawiedliwością legalną (prawną), nakazująca miłość ojczyzny, cenienie bardziej jej dobra wspólnego od interesów osobistych czy partykularnych, współtworzenie jej kultury materialnej i umysłowo – aksjologicznej, w razie konieczności jej obronę, w każdy możliwy sposób”[15]. Sprowadzając patriotyzm do prostej definicji jest to „miłość ojczyzny i przywiązanie do swojego narodu”[16], przy czym, co należy podkreślić, miłość ta i przywiązanie z jednej strony objawiają się poprzez „prymat dobra wspólnego oraz interesu publicznego nad osobistą korzyścią człowieka”[17], z drugiej związane są z „nakazem poszanowania innych narodów i pokojowej z nimi współpracy”[18]. Patriotyzm nie tylko pociąga za sobą dobrowolnie przyjęte obowiązki, tj.:[19] przynależność do społeczności narodowej stanowiącej ojczyznę, szanowanie jej dobrego imienia i wierność,

[10] F. Koneczny*, O ład w historii*, Dom Wydawniczy Ostoja, Krzeszowice 2013, s. 31.
[11] K. Chałas, A. Maj (red.), *Encyklopedia aksjologii pedagogicznej…*, op. cit., s. 680.
[12] Ibidem, s. 681.
[13] F. Koneczny*, O ład w historii…*, op. cit., s. 31.
[14] K. Chałas, A. Maj (red.), *Encyklopedia aksjologii pedagogicznej…,* op. cit., s. 680.
[15] Ibidem, s. 729.
[16] Mały słownik języka polskiego…, op. cit., s. 543.
[17] K. Chałas, A. Maj (red.), *Encyklopedia aksjologii pedagogicznej…,* op. cit., s. 729.
[18] Ibidem, s. 732.
[19] Ibidem, s. 730.

pielęgnowanie języka, kultury, znajomość historii, kultywowanie tradycji, rzetelna praca, posłuszeństwo wobec prawowitej władzy respektującej prawa człowieka, współodpowiedzialność za ład społeczno – moralny oraz dobro wspólne, aż po gotowość do czynnej obrony suwerenności oraz integralności kraju, ale stanowi również „kryterium poczucia narodowego”[20].

Poczucie narodowe nie zaistnieje jednak bez narodu, którego stanowi istotną cechę, a na które składa się m.in.: „przeświadczenie o pochodzeniu od wspólnych przodków, świadomość i zgodna ocena wspólnych dziejów, poczucie wspólnych interesów życiowych w chwili teraźniejszej i na przyszłość (…) wzajemna życzliwość i przychylność członków zbiorowości oraz przywiązanie do niej”[21]. Naród zaś jest „zrzeszeniem cywilizacyjnym posiadającym ojczyznę i język ojczysty”[22], a przynależność do niego ma charakter dobrowolny. Narodowość wytwarza się historycznie, jest „wytworem pracy, nabytkiem rozwoju, świadectwem udoskonalenia, do którego doszło się ciężkim trudem pokoleń, wśród walk, bólów, zawodów, ale też z myślą przewodnią, mającą wieść do coraz wyższego udoskonalenia tego materiału etnologicznego, który historia zebrała w naród przez dostojeństwo pracy kulturalnej”[23]. Naród jest zatem rozumiany jako wspólnota jego członków, dla której ważne są pewne wartości, związane z tradycją wspólnych losów, językiem, elementami kultury, a także z dążeniem do zachowania ich odrębności, co stanowi fundament do trwania i rozwoju poprzez umacnianie świadomości narodowej[24].

Tam, gdzie państwo oparte jest na społeczeństwie, społeczeństwo stanowi fundament zarówno państwa, jak i narodu, w taki sposób, że państwo stanowi prawną nadbudowę społeczeństwa, podczas gdy naród, etyczną[25]. Wydaje się zatem, że można by przyjąć, iż naród i społeczeństwo to synonimy, które występuję zamiennie, a ich substytucja definiuje równorzędne pojęcia, jako że oba słowa określają wspólnotę, ogół. W kontekście bezpieczeństwa państwa jest to jednak uproszczenie, które nie oddaje istoty sprawy i nie eksponuje zasadniczej różnicy między nimi.

[20] F. Koneczny, *Polskie logos a ethos. Roztrząsania o znaczeniu i celu Polski*, Cyfrowa Biblioteka Myśli Narodowej, s. 171, https://cbmn.pl/feliks-koneczny/polskie-logos-a-ethos, [dostęp: 14.03.2025].

[21] W. Kitler, *Bezpieczeństwo narodowe RP…*, op. cit., s. 16.

[22] F. Koneczny, *O wielości cywilizacji*, Capital sp. z o.o., Warszawa 2015, s. 392.

[23] Ibidem, s. 388.

[24] Cz. Mojsiewicz (red.), *Leksykon współczesnych międzynarodowych stosunków politycznych*, Wydawnictwo Atla 2, Wrocław 1997, s. 215.

[25] F. Koneczny, *O wielości cywilizacji*…, op. cit., s. 387.

Społeczeństwo bowiem, jest to „ogół ludzi pozostających we wzajemnych stosunkach wynikających z ich udziału w procesach produkcyjnych”[26], inaczej „ogół obywateli danego kraju, okręgu, miasta”[27]. Cechą społeczeństwa jest „pewien stopień trwałej odrębności od innych zbiorowości tego rodzaju i względna intensywność wzajemnych oddziaływań pomiędzy jego członkami, połączonymi przez wspólne terytorium, instytucje, ustalone sposoby komunikowania się, podobieństwo warunków życia, podział pracy, normy i wzorce postępowania”[28], co nie musi być bynajmniej jednoznaczne i tożsame ze zbiorowością o wspólnych: dziejach, tradycji, kulturze, języku czy religii. Szczególnie widoczne jest to w społeczeństwach współczesnych, złożonych z różnych społeczności. Zasadniczą różnicę między społeczeństwem a narodem stanowi zatem wspólna świadomość narodowa, poczucie przynależności do wspólnoty danego narodu, stanowiącego wspólnotę idei i emocji[29], czyli właśnie poczucie narodowe. Bez tej nadbudowy członkowie społeczeństwa mogą równie dobrze zmierzać w kierunku kosmopolityzmu, który cechuje się obojętnością na kwestie ojczyzny i własnego narodu oraz brakiem poczucia współodpowiedzialności za ich sprawy.

To wiąże się z pojęciem dobra wspólnego (łac. *bonum commune*), jako kategorii związanej z życiem społecznym człowieka. Dobro wspólne oznacza ogół czynników materialnych (dobra doczesne) oraz duchowych (wartości religijne, moralne, intelektualne, artystyczne, estetyczne), które są niezbędne do osiągnięcia przez określoną wspólnotę dobrobytu, który sprzyja harmonijnemu rozwojowi tej wspólnoty[30]. Pojęcie to definiowane jest jako podstawowy czynnik życia społecznego, rzeczywisty cel pojedynczego człowieka, jak i społeczności, który stanowi uzasadnienie i przesłankę istnienia, jak i powstania tej społeczności, a także czynnik motywujący aktywność społeczną tworzących daną społeczność jednostek[31]. Dobro indywidualne, wywodząc z powyżej definicji, wiąże się zatem z tworzeniem takich warunków, które będą sprzyjały harmonijnemu i integralnemu rozwojowi osoby ludzkiej, w jakich będzie mogła się realizować w kierunku osiągnięcia własnej doskonałości z poszanowaniem jej praw i obowiązków. Dobro wspólne jako wartość zbiorowa,

[26] *Mały słownik języka polskiego…*, op. cit., s.767.
[27] Ibidem.
[28] *Wielka Encyklopedia PWN…*, t. 25, op. cit., s. 446.
[29] Ibidem, t. 18, s. 355.
[30] K. Chałas, A. Maj (red.), *Encyklopedia aksjologii pedagogicznej…,* op. cit., s. 260.
[31] Ibidem, s. 261.

wytwarza się zatem poprzez rozwijanie naturalnych zdolności i możliwości, zaspokajanie indywidualnych interesów i potrzeb, respektowanie posiadanych przez jednostkę uprawnień, idące w parze z jednoczesną, świadomą dbałością o „zbliżanie całej wspólnoty ku właściwym jej celom”[32].

Bezpieczeństwo, w tym bezpieczeństwo państwa

Bezpieczeństwo było, jest i będzie jedną z podstawowych potrzeb zarówno jednostki, jak i społeczeństwa. Stanowi, zaraz po konieczności zaspokojenia potrzeb fizjologicznych, kolejny, ale wciąż elementarny poziom, złożony ze zbioru czynników, których brak zaburza, a wręcz uniemożliwia funkcjonowanie i rozwój tak pojedynczej osoby, jak i określonej zbiorowości[33].

Bezpieczeństwo w najprostszy sposób można zdefiniować jako brak zagrożeń, spokój, pewność, gwarancję, ochronę, jak również - wynikającą z powyższych elementów, tworzących jednocześnie warunek sine qua non jej zaistnienia - perspektywę rozwoju[34]. Bezpieczeństwo stanowi zatem z jednej strony przyczynę podejmowanych przez człowieka działań, występując w tym kontekście w roli czynnika motywującego, jak również z drugiej, ich skutek, gdy w wyniku podjętej aktywności stanowi jej efekt i rezultat. Ten ciąg przyczynowo - skutkowy, który jawi się procesem constans, zapewnia - zarówno w wymiarze jednostki, wspólnoty, jak i państwa - przetrwanie, integralność, leży u podstaw wzrostu, przekłada się bezpośrednio na suwerenności, niepodległości oraz wolności podmiotu.

Jednocześnie, ów ciąg przyczynowo – skutkowy, będący procesem ciągłym, nie stanowi bynajmniej modelu perpetuum mobile. Koncentrując się na bezpieczeństwie państwa, nie jest bowiem wystarczającym jedynie określić działania na rzecz bezpieczeństwa, zainicjować ich wdrożenie i jednorazowym aktem wprowadzić w czyn. Dzieje się tak nie tylko z uwagi na zmieniające się okoliczności, zagrożenia, dynamikę zjawisk i zdarzeń, warunki wewnętrzne oraz zewnętrzne, oddziałujące na stan bezpieczeństwa, ale też ze względu na ulegające zmianom zasoby w znaczeniu sensu largo: materialne, niematerialne, osobowe, stanowiące o potencjale bezpieczeństwa państwa, rozumianego jako troska o zachowanie ładu publicznego, czy ochrona przed

[32] *Wielka Encyklopedia PWN…*, op. cit., t. 7, s. 233.

[33] Hierarchia potrzeb Abrahama Maslowa.

[34] A. Szczepański, *Pojęcie bezpieczeństwa i jego typologia – próba systematyzacji*, Zeszyty Naukowe Collegium Witelona, nr 48(3), 2023, s 28-30.

zagrożeniami zewnętrznymi np.: w kontekście integralności terytorialnej, przetrwania narodu[35].

O ile potrzeba bezpieczeństwa człowieka jest rzeczą bezsporną, podobnie zresztą jak potrzeba bezpieczeństwa państwa, o tyle pojawia się pytanie, czy można obu tym potrzebom przypisać taką samą lub zbliżoną wagę, z punktu widzenia jednostki, czy też danego społeczeństwa. Jeśli bowiem przyjmiemy, że potrzeba bezpieczeństwa jest ściśle związana z występowaniem trzech czynników, tj.: podmiotu (człowiek, społeczeństwo, państwo), wartości (na ile podmiot postrzega coś jako dobro, na ile jest to dla niego ważne) oraz zagrożenia (prawdopodobieństwo utraty tego dobra), co określone zostało jako tzw.: trójkąt bezpieczeństwa[36], oczywistym staje się, że czynnik subiektywny odgrywa znaczącą rolę. Ponadto, jeśli warunkiem sine qua non jest jednoczesne współistnienie wszystkich elementów owej triady, w innym bowiem przypadku potrzeba bezpieczeństwa nie zaistnieje[37], odpowiedź na wyżej postawione pytanie, nie jest ani jednoznaczna, ani nie można postrzegać jej w kategoriach uniwersalnych. Głównym powodem tego jest oczywiście kwestia wartości, czyli perspektywa, postrzeganie, co dla kogo przedstawia wartość i jak duże dobro stanowi. W aspekcie bezpieczeństwa państwa ma to istotne znaczenie.

Kolejną zmienną, oprócz czynnika subiektywnej oceny, mającą znaczenie dla bezpieczeństwa państwa jest wiedza, która przekłada się na świadomość lub brak świadomości jednostki, a w konsekwencji ogółu społeczeństwa, dotycząca prawdopodobieństwa pojawienia się zagrożenia, już istniejącego zagrożenia oraz znaczenia tego zagrożenia, czyli tzw.: powagi sytuacji, w ujęciu obiektywnym. Korelacje pomiędzy stanem świadomości danego podmiotu a jego subiektywną oceną określonego stanu rzeczy, w tym przypadku zagrożenia, sformułował Daniel Frei, który wyróżnił cztery poziomy ilustrujące stan bezpieczeństwa: stan braku bezpieczeństwa, stan obsesji, stan fałszywego bezpieczeństwa, stan bezpieczeństwa[38].

Jedynie zgodność sądu z rzeczywistym stanem rzeczy[39], daje nam nie tylko właściwy obraz rzeczywistości, ale też pozwala przedsięwziąć właściwe

[35] W. Kitler, *Bezpieczeństwo narodowe RP*…, op. cit., s. 28.

[36] J. Piwowarski, *Nauki o bezpieczeństwie. Kultura bezpieczeństwa i redefinicja środowiska bezpieczeństwa*, Wydawnictwo Difin, Warszawa 2020, s. 25.

[37] Ibidem, s. 26.

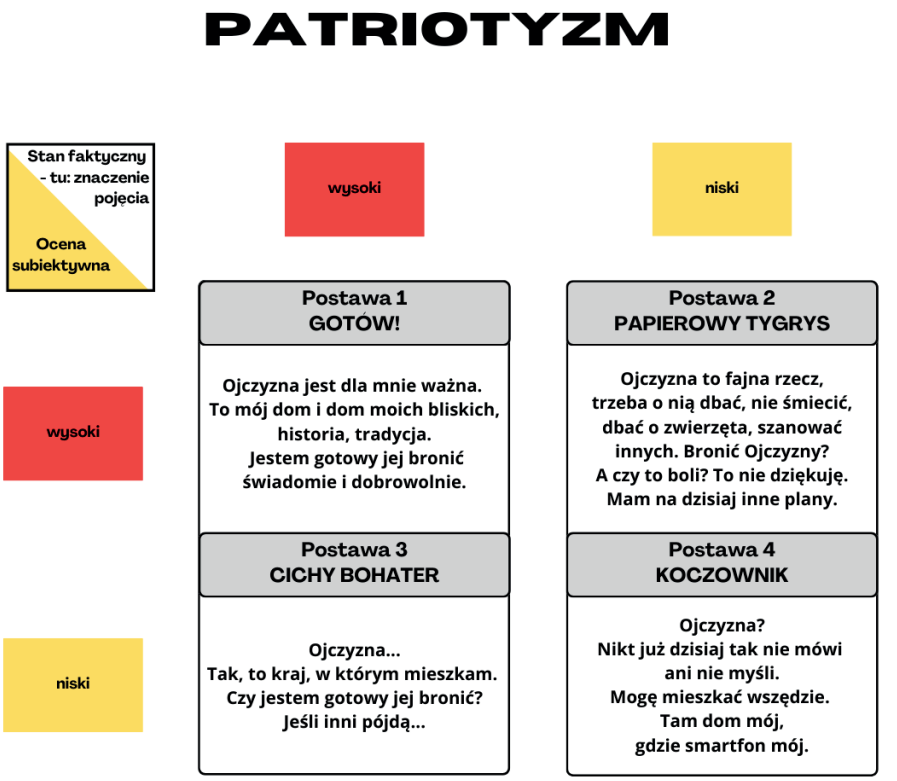
[38] Ibidem, s. 56.

[39] Jest to równocześnie definicja prawdy według Arystotelesa.

kroki. W sytuacji, gdy siła i kierunek wzajemnych powiązań obu zmiennych (percepcja, osąd) rozchodzą się lub są przeciwstawne, nie tylko nie jest to zgodne z prawdą, ale też implikuje określone skutki, tj.: podjęcie niewłaściwych decyzji, działań lub zaniechanie podjęcia właściwych decyzji i działań. Model Daniela Freia odnosi się wprost do poczucia bezpieczeństwa podmiotu, jakim jest jednostka. Można jednak spróbować zastosować go do oceny stanu czy też potencjału bezpieczeństwa państwa, przyjmując, że podmiotem jest wciąż osoba, ale w miejsce zagrożenia postawione zostaną wartości ważne z punktu widzenia bezpieczeństwa państwa, tj.: patriotyzm, poczucie narodowe, dobro wspólne.

Zestawiając ze sobą subiektywne postrzeganie oraz rozumienie przez jednostkę konkretnych pojęć, jako świadomość lub brak świadomość ich znaczenia, czy też zróżnicowany poziom tej świadomości, czy też rozumienia, ze stanem rzeczywistym, czyli definicją, właściwym znaczeniem, istotą danego pojęcia, o czym była mowa w punkcie pierwszym niniejszego opracowania, można podjąć próbę określenia wynikających z tych korelacji postaw. Przebadanie pod tym kątem społeczeństwa lub wybranych grup, mogłoby stanowić pewne narzędzie do określenia stanu lub potencjału bezpieczeństwa państwa, w tym jego zdolności obronnych, jak również rozwojowych.

Analizując pojęcie patriotyzmu, w kontekście wartości, ważnego dla podmiotu dobra, wyłaniają się cztery postawy: *Gotów!, Papierowy Tygrys, Cichy Bohater oraz Koczownik*. Ich charakterystykę przedstawiono na rysunku 1.



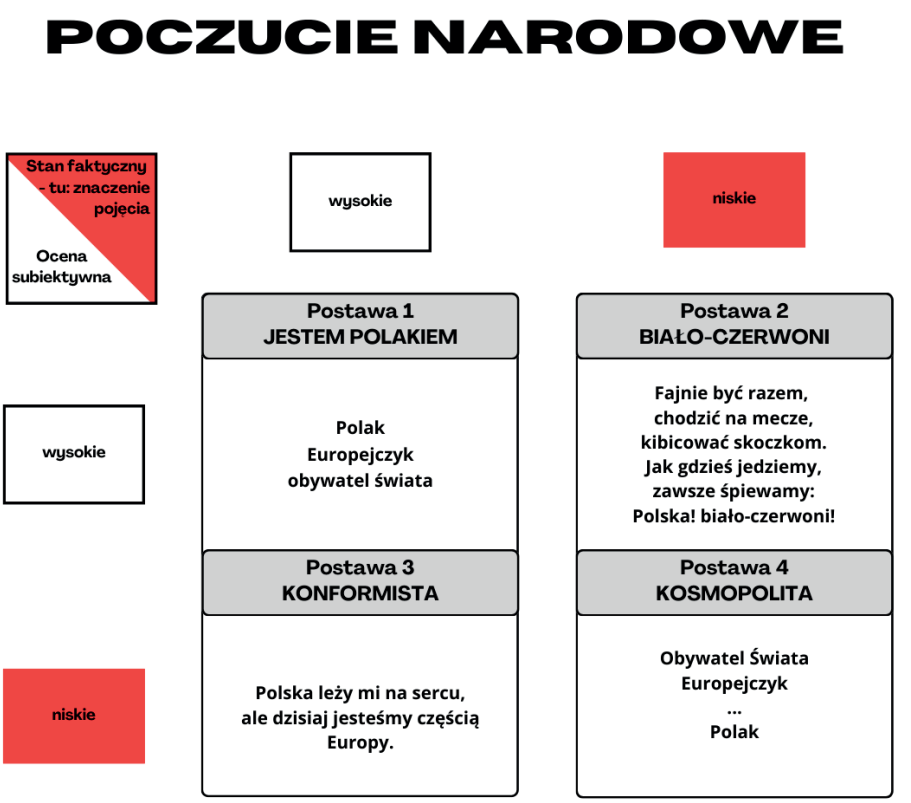
Rysunek 1. Pojęcie patriotyzmu i wynikające z tego postawy w kontekście bezpieczeństwa państwa

Źródło: opracowanie własne w oparciu o model Daniela Frei'a.

Postawa *Gotów!* jest najbardziej pożądaną z punktu widzenia bezpieczeństwa państwa. Jeśli bowiem ojczyzna nie jest pustym słowem, ale przedmiotem godnym troski, wierności i poświęceń, mogącym nadawać sens ludzkiej egzystencji oraz poczucie przynależności, patriotyzm jest wówczas czymś naturalnym, niewymuszonym i przekłada się na pełną gotowość do obrony ojczyzny w przypadku zagrożenia, czy też podejmowanie na co dzień mądrych decyzji oraz skutecznych działań na rzecz dobra i rozwoju kraju, a tym samym rodaków. Na przeciwnym biegunie znajduje się postawa nazwana *Koczownik*, która odzwierciedla brak przywiązania do ziemi, gotowość do zmiany miejsca pobytu. Postawa ta reprezentuje wyłączną troskę o dobro własne i natychmiastową ewakuację z miejsca zagrożenia. Niestety niskie poczucie więzi ze swoim krajem przekłada się również na niskie zaangażowanie w dbałość o dobro tego kraju i poczucie odpowiedzialności za jego sprawy i los. Kolejne dwie postawy: *Tekturowy Tygrys i Cichy Bohater* są przykładami

osób, w świadomości których istnieje pojęcie ojczyzny, jako dobra. Jednak może być albo zbyt powierzchownie rozumiane albo w ogóle nie stanowiące przedmiotu głębszych przemyśleń. Są to postawy poniekąd niedookreślone, które w obliczu zagrożenia mogą obrać różny kierunek.

Podobne zależności można zauważyć analizując poczucie narodowe, ściśle związane z pojęciem narodu oraz poczuciem bycia jego częścią w oparciu o wspólne wartości.Jak postrzeganie tej przynależności i utożsamianie się z tym, a nie innym narodem, w zestawieniu z rzeczywistym znaczeniem tego pojęcia, przekłada się na postawę człowieka w aspekcie bezpieczeństwa państwa przedstawia rysunek 2. Tożsamość człowieka, czyli świadomość tego kim jest, skąd pochodzi i dokąd zmierza, implikuje to, jak określa samego siebie w stosunku do własnej oraz innych nacji. Postawa *Kosmopolity*, Obywatela świata przez duże „O", z racji rozmiaru globu ogranicza w znacznym stopniu miejsce na polskość i daje nikłą nadzieję ojczyźnie na wsparcie w potrzebie, czy też społeczeństwu polskiemu na rozwój. Może się to przejawiać poprzez porzucanie rodzimych tradycji, nieprzywiązywanie wagi do pamięci historycznej, a w zamian przyjmowanie zwyczajów i narracji innych nacji. Postawa *Jestem Polakiem*, oparta na właściwym rozumieniu i uchwyceniu istoty pojęcia, wręcz odwrotnie. Stanowi trzon i zaczyn bezpieczeństwa państwa, jego dobra i wzrostu. Podobnie, jak w przypadku patriotyzmu, dwie środkowe postawy: *Biało-czerwoni* oraz *Konformista* stanowią pewien potencjał, który, w interesie bezpieczeństwa państwa, wymaga uwagi, jak również zagospodarowania, zaopiekowania, poprzez pogłębianie świadomości, a być może nawet zbudowanie lub przywrócenie właściwej wartości i znaczenia pojęciu poczucia narodowego.

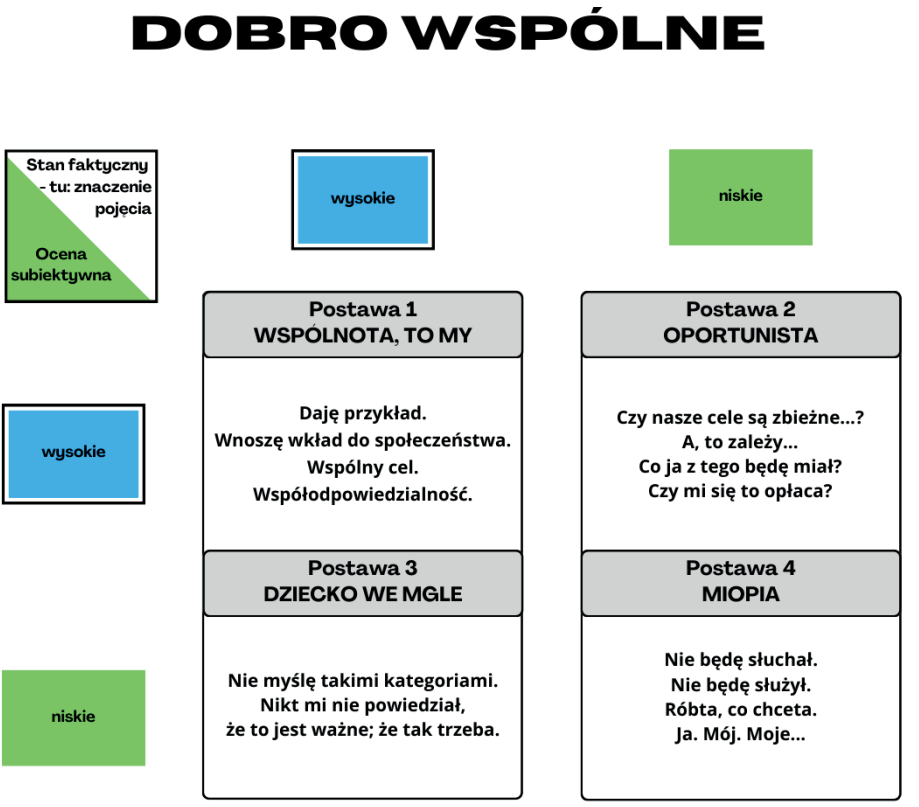


Rysunek 2. Pojęcie poczucia narodowego i wynikające z tego postawy w kontekście bezpieczeństwa państwa

Źródło: opracowanie własne w oparciu o model Daniela Frei'a.

Poczucie narodowe jako przynależność do określonej wspólnoty determinuje również stosunek do bonum commune. Rysunek 3 przedstawia przykładowe postawy w zależności od relacji pomiędzy osobistym osądem, a rzeczywistym stanem rzeczy.

Z niniejszego schematu, podobnie jak w pozostałych przypadkach, wyłaniają się dwie postawy przeciwstawne oraz dwie niedookreślone w kontekście bezpieczeństwa państwa. Postawa *Wspólnota, to My* cechuje się wysoką świadomością znaczenia dobra wspólnego, co przekłada się na wzięcie odpowiedzialności i podejmowanie decyzji i działań, które służą nie tylko dobru indywidualnemu, ale także wspólnocie, jaką jest rodzina, środowisko pracy, środowisko lokalne, a w konsekwencji naród i państwo polskie.



Rysunek 3. Pojęcie dobra wspólnego i wynikające z tego postawy w kontekście bezpieczeństwa państwa

Źródło: opracowanie własne w oparciu o model Daniela Frei'a.

Podejście zgoła odmienne, nazwane pojęciem medycznym oznaczającym krótkowzroczność, koncentruje się wyłącznie na dobru własnym. Osoba reprezentująca postawę *Miopia,* działania i decyzje podejmuje przez pryzmat osiągnięcia własnego dobrostanu, rozumianego jako „subiektywnie postrzegane przez osobę poczucie szczęścia, pomyślności, zadowolenie ze stanu życia"[40], życia tu i teraz, bez oglądania się na innych. Jest to na ogół postawa egoistyczna, niezdolna do poświęceń. *Oportunista* będzie wysoko cenił różne akcje charytatywne, zbiórki, wydarzenia dające mu poczucie działania na rzecz dobra wspólnego, a w rzeczywistości zaspokajające jego własne potrzeby i osiąganie korzyści, np.: w postaci uznania czy prestiżu społecznego. Ostatnia postawa, *Dziecko we mgle,* żyje w nieświadomości znaczenia swojego wkładu

[40] sjp.pwn.pl//szukaj/dobrostan.html, [dostęp: 19.03.2025].

na rzecz dobra wspólnego, ale ma w rzeczywistości potencjał, który może się rozwinąć i zaprocentować.

Podsumowując, nasuwają się następujące wnioski. Patriotyzmu nie da się odczuwać w stosunku do państwa. Jest on bowiem związany z pojęciem ojczyzny. Podobnie, poczucia narodowego nie łączy się z pojęciem społeczeństwa, ale narodu – wspólnoty, którą łączy ojczyzna, język, tradycja. Natomiast bez ojczyzny i narodu wartość i znaczenie dobra wspólnego, wydają się wtórne w stosunku do dobra indywidualnego, gdyż to właśnie te pojęcia tworzą wspólny mianownik, a tym samym spoiwo łączące jednostkę z ogółem. Powyższych pojęć, jak i innych, ważnych z punktu widzenia bezpieczeństwa państwa czy bezpieczeństwa narodowego, nie uda się pojmować w charakterze wartości, stanowiących dobro bez ukształtowanych, właściwych postaw obywateli.

Kształtowanie postaw

Kształtowanie, inaczej formowanie, stanowi zasadniczy element wychowania, które będąc procesem złożonym, jest przedmiotem zainteresowań, jak i obszarem badań różnych nauk i dziedzin, przez co posiada szereg definicji. Na potrzeby niniejszego opracowania przyjęto definicję wychowania podaną w Słowniku języka polskiego jako „ogół zabiegów mających na celu ukształtowanie człowieka pod względem fizycznym, moralnym i umysłowym oraz przygotowanie go do życia w społeczeństwie”[41], ale przy założeniu, iż zabiegi te mają charakter „wspierający rozwój człowieczeństwa dziecka”[42]. Postawa natomiast to zarówno „stosunek człowieka do życia lub do pewnych zjawisk, wyrażający jego poglądy”, jak również „sposób postępowania lub zachowania wobec określonych zjawisk, zdarzeń lub w stosunku do ludzi”[43]. Kształtowanie postaw zawiera się zatem w oddziaływaniu na człowieka, w celu przyjęcia przez niego określonych norm moralnych, nabycie cnót[44], które będą determinować jego decyzje i działanie w określonych sytuacjach. Ważne są dlatego

[41] sjp.pwn.pl/szukaj/wychowanie.html, [dostęp: 28.03.2025].

[42] K. Chałas, A. Maj (red.), *Encyklopedia aksjologii pedagogicznej*…, op. cit., s. 1368.

[43] sjp.pwn.pl/szukaj/postawa.html, [dostęp: 28.03.2025].

[44] Cnota rozumiana jest jako osobowa cecha człowieka, sprawność do działania ku dobru; skłonność, sprawność do spełniania aktów moralnie dobrych – por. K. Chałas, A. Maj (red.), *Encyklopedia aksjologii pedagogicznej*…, s. 169 i 181.

zarówno cel, skala oddziaływania, trwanie tego oddziaływania w czasie, jak również spójność.

Zakładając, że jednym z efektów kształtowania postaw, czy, w pewnym sensie, celem pośrednim, jest bezpieczeństwo państwa, rozumiane jako jego integralność, przetrwanie i rozwój, istotnym staje się podjęcie wysiłku eksponowania i rozwijania cnót, zarówno rozumu, jak i etycznych oraz społecznych[45], które celowi temu będą służyć przy równoczesnym podjęciu trudu eliminowania wad, które są owych cnót przeciwieństwem. Proces ten powinien być realizowany długookresowo, a więc w okresie rozwoju i dorastania dziecka, jak również sukcesywnie i systemowo, a zakończyć się przejściem od wychowania do świadomego samowychowania, które jest „obowiązkiem każdego dorosłego człowieka"[46]. Niezwykle ważna jest skala oddziaływania, rozumiana jako ogół podmiotów mających wpływ na kształtowanie postaw: dom, szkoła, środowisko, kościół, a więc rodzice, nauczyciele, sąsiedzi, osoby duchowne, organizacje, instytucje, kluby etc. Istotnym czynnikiem są również szeroko rozumiane media, szczególnie nowe media[47], których udział w procesie formowania poglądów oraz systemu wartości – poprzez dużą ilość czasu spędzanego w nich przez coraz mniejsze dzieci, a przez to rozluźnienie więzi z rodzicami, czy obecność w nich influencerów, jako nowych autorytetów - bynajmniej nie jest marginalny[48]. Przesunięcie punktu ciężkości z modelu wychowania, w którym wychowawca (rodzic, nauczyciel, trener,

[45] Do cnót rozumu zaliczane są: poznanie naukowe, rozumienie, mądrość, rozumne działanie i wytwarzanie, roztropność. Do cnót etycznych zalicza się: umiarkowanie (którego częścią integralną jest m.in.: godność, wyrozumiałość, skromność), męstwo (którego częścią integralną jest m.in.: zaufanie, cierpliwość, wytrwałość, wielkoduszność), sprawiedliwość (której częścią integralną jest m.in.: czynienie dobra, unikanie zła, a do składników zaliczane są m.in.: posłuszeństwo, karność, prawdomówność, ofiarność, patriotyzm, miłość do najbliższych, cześć wobec społeczności, w której się wyrosło, szacunek wobec innych oraz wobec własności prywatnej i narodowej). Sprawiedliwość, przyjaźń i miłość wymieniane są również jako cnoty społeczne - por. K. Chałas, A. Maj (red.), *Encyklopedia aksjologii pedagogicznej…,* op. cit., ss. 168-209.

[46] E. Ozimek (red.), *Wychowanie – potrzeba dziecka – zadanie domu i szkoły*, Oficyna Współczesna, Poznań 1999, s. 39.

[47] Do nowych mediów zalicza się m.in. strony internetowe, pocztę elektroniczną, społeczności internetowe, reklamę internetową, kioski elektroniczne, aparaty i kamery cyfrowe, integrację cyfrowych danych z telefonu, środowiska wirtualnej rzeczywistości (w tym gry wideo) - por. Główny Urząd Statystyczny, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1943,pojecie.html, [dostęp: 28.03.2025].

[48] A. Wiejak, *Cyberrewolucja. Nowy totalitaryzm*, Wydawnictwo AA s.c., Kraków 2025, s. 31.

ksiądz) oddziałuje na wychowanka w sposób bezpośredni na model, w którym wychowanie odbywa się przy wykorzystaniu technologii informacyjno – komunikacyjnych, niesie za sobą niebezpieczeństwo, że poza wiedzą i kontrolą wychowawców pozostaną odbierane przez wychowanków przekazy – ich jakość i treść, a przez to powstaje ryzyko braku spójności pomiędzy celami wychowawczymi, a czasami wręcz ich rozbieżność. Spójność jest natomiast jednym z kluczowych elementów kształtowania postaw, a zachowana w dłuższym okresie, przekłada się na ich trwałość, prowadzi nie tylko do przyjęcia danego pojęcia na poziomie poznawczym, ale przede wszystkim głębokiego zrozumienia i wewnętrznej asymilacji, co pozwala ukształtować spójny system wartości. Siłę i trzon formowania postaw stanowi współdziałanie i uzupełnianie się rodziców, nauczycieli, wychowawców w wypełnianiu ich roli wychowawczej i edukacyjnej oparte na jednym systemie wartości. Jedność w działaniu i przekazywanie spójnych treści stanowi nieodzowny warunek, by osiągnąć wysoką efektywność i pożądane efekty: komplementarny, wszechstronny i integralny rozwój człowieka[49].

Ważnym jest zatem, by nieustannie nauczać, przypominać, dawać przykład, a przede wszystkim dążyć do zaangażowania jak największej liczby osób i podmiotów pracujących na rzecz kształtowania właściwych postaw ukierunkowanych, a wręcz dających gwarancję troski i staranności o bezpieczeństwo państwa, widzenia w nim wspólnego celu i najwyższego dobra. Niewystarczającym jest zatem sama obecność tematyki bezpieczeństwa w dyskursie publicznym, czy też organizowanie szkoleń, których przedmiotem jest pewien proces mechaniczny, to znaczy zorientowany stricte na umiejętności tj.: obsługa broni, rzut granatem czy udzielenie pierwszej pomocy etc.

Bezpieczeństwo państwa, bez zbudowania wcześniej fundamentu w postaci zaszczepienia właściwych pojęć, może być, z punktu widzenia pojedynczego obywatela, zajętego na co dzień własnymi, bieżącymi sprawami, traktowane jako zadanie służb, polityków, podmiotów zajmującym się tematyką bezpieczeństwa profesjonalnie, ale niedotyczące go w sposób bezpośredni. W konsekwencji, w dłuższej perspektywie, może to prowadzić nie tylko do bierności, ale też zupełnego braku świadomości własnej roli, czego wynikiem będzie brak identyfikowania siebie jako podmiotu mającego wpływ i znaczenie w tym nieustającym procesie i ciągu przyczynowo – skutkowym.

[49] M. Bobro (red.), *Etos pracy nauczyciela w oparciu o myśl chrześcijańsko – społeczną*, Wydawnictwo Naukowe ArcheaGraph, Łódź-Warszawa, 2024, s. 76.

By uniknąć takiego podejścia, czy też wyeliminować postawę bycia obserwatorem, a nie uczestnikiem, będącym częścią procesu zapewnienia bezpieczeństwa państwa, konieczna jest świadomość i zaangażowanie. Te zaś powstają nie tylko w wyniku rozwijania procesów poznawczych poprzez nauczanie, ale w wyniku wychowania, tj.: kształtowania właściwych postaw prowadzących do odkrywania własnej tożsamości, a przez to systemu wartości, w którym pojęcia takie jak: ojczyzna, naród, dobro wspólne, będą zajmowały poczytne miejsce, co w konsekwencji będzie implikować przemyślane, skuteczne, zasadne, proporcjonalne działania lub zaniechanie działań niezasadnych, nieskutecznych, nieadekwatnych, czyli profilaktykę, prewencję.

Wspólnota złożona z takich jednostek stanowi niewątpliwie filar bezpieczeństwa państwa, które to bezpieczeństwo buduje się na poziome podejmowania mądrych decyzji, by nie dopuszczać do pojawienia się zagrożeń prowadzących do konieczności chwycenia za broń, ale by gotowość na to, w sytuacji bez wyjścia, była dobrowolna i wynikająca z potrzeby serca.

Podsumowanie

Żyjąc jedynie w obrębie pojęć: państwo, społeczeństwo czy dobro indywidualne, pojmowane jako dobrostan, bez osadzenia tych pojęć na osi uniwersalnych wartości, istnieje niebezpieczeństwo rozmycia a nawet utraty tożsamości oraz zaniku więzi z własnym krajem, językiem, tradycją, historią. Może to skutkować obojętnością nie tylko na sprawy wewnętrzne, ale też politykę zewnętrzną, czy integralność granic. Kolejność kształtująca hierarchię pojęć: Polak – Europejczyk – obywatel świata versus obywatel świata – Europejczyk – Polak, ma znaczenie w postrzeganiu swojego kraju oraz własnej roli dla rozwoju i ochrony tego kraju. Może się bowiem przełożyć na opinie i postawy, że wszystko jedno, gdzie kto będzie mieszkał, pracował, żył, byleby było względnie bezpiecznie, nierzadko w rozumieniu, wygodnie.

W dobie globalizacji, której jednym z elementów jest zacieranie różnic kulturowych[50] oraz społeczeństwa informacyjnego, definiowanego przez Jerzego Kisielnickiego, jako „takie społeczeństwo, które posiada dostęp i umie wykorzystać: informatyczną infrastrukturę, zasoby informacji i wiedzy dla realizacji

[50] sjp.pwn.pl/szukaj/globalizacja.html, [dostęp: 19.03.2025].

zbiorowych i indywidualnych celów w sposób skuteczny i ekonomiczny”[51] oraz - jak wskazuje Wielka Encyklopedia Internetu i Nowych Technologii - społeczeństwo, „w którym najważniejszym czynnikiem kształtującym świadomość i gospodarkę jest informacja; dostęp do informacji oraz umiejętność korzystania z nowoczesnych technologii i środków przekazu (przede wszystkim globalnej sieci) jest w takim społeczeństwie najwyższym dobrem”[52], wydaje się, że – z punktu widzenia bezpieczeństwa państwa – rozeznanie znaczenia pojęć i różnicy między nimi jest kluczowe.

Przypominać należy, że dobrem wspólnym wszystkich obywateli jest Rzeczpospolita Polska[53], która jest państwem jednolitym[54], w którym władza zwierzchnia należy do Narodu[55], którego członkowie, jako obywatele polscy mają obowiązek obrony Ojczyzny. Bez głębokiego zrozumienia pojęć tj.: naród, ojczyzna, patriotyzm, poczucie narodowe, dobro wspólne i bez uczynienia ich elementem systemu wartości tworzących tożsamość człowieka; bez uczynienia ich znaczenia ważnymi, wartymi troski, wierności, poświęcenia, budowanie bezpieczeństwa państwa nie będzie ani kompletne, ani skuteczne. Wspólnym mianownikiem, a jednocześnie spoiwem i czynnikiem nadającym właściwe znaczenie powyższym pojęciom, a także właściwe ich miejsce w duszy człowieka, jest bowiem jasne poczucie tożsamości, czyli świadomość kim jestem, skąd pochodzę, dokąd zmierzam. Świadomość ojczyzny jako wspólnego dobra wszystkich obywateli – Narodu, którego poczucie narodowe członków i ich patriotyzm stanowią o jego sile przetrwania, rozwoju i gwarancji bezpieczeństwa państwa, jest bezcenna. Uczynić to można jedynie poprzez edukację na rzecz bezpieczeństwa już od najmłodszych lat, tym bardziej, że „miłość Ojczyzny nie zawsze jest i nie dla wszystkich jest uczuciem wrodzonym; ona jest cnotą i jak każdej cnoty trzeba się jej uczyć i do niej wprawiać”[56],

[51] P. Sienkiewicz, J. S. Nowak (red.), *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, Polskie Towarzystwo informatyczne – Oddział Górnosląski, Katowice 2008, s. 15, https://delibra.bg.polsl.pl/Content/24504/BCPS_27164_2006_Spoleczenstwo-inform.pdf, [dostęp: 19.03.2025].

[52] Ibidem.

[53] Konstytucja Rzeczypospolitej Polskiej…, op. cit., Art. 1.

[54] Ibidem, Art. 3.

[55] Ibidem, Art. 4 ust. 1.

[56] J. Zamoyska, *Myśli wybrane*, Fundacja Servire Veritati Instytut Edukacji Narodowej, Lublin 2013, s. 92.

a „poświęcenie jest tak od miłości nierozdzielne, tak z niej wynika, że nie można mówić o miłości Ojczyzny, żeby nie mówić o służbie dla Ojczyzny”[57].

Literatura

1. Chałas K., Maj A. (red.), *Encyklopedia aksjologii pedagogicznej*, Polskie Wydawnictwo Encyklopedyczne, Radom 2016.
2. Główny Urząd Statystyczny, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1943,pojecie.html.
3. Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie Uwarunkowania System*, Akademia Obrony Narodowej, Warszawa 2011.
4. Koneczny F., *O ład w historii*, Dom Wydawniczy „Ostoja”, Krzeszowice 2013.
5. Koneczny F., *Polskie logos a ethos. Roztrząsania o znaczeniu i celu Polski*, Cyfrowa Biblioteka Myśli Narodowej, (https://cbmn.pl/feliks-koneczny/polskie-logos-a-ethos).
6. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 Nr 78, poz. 483).
7. Mały słownik języka polskiego, Państwowe Wydawnictwo Naukowe, Warszawa 1969.
8. Mojsiewicz Cz. (red.), *Leksykon współczesnych międzynarodowych stosunków politycznych*, Wydawnictwo altla 2, Wrocław 1997.
9. Ozimek E. (red.), *Wychowanie – potrzeba dziecka – zadanie domu i szkoły*, Oficyna Współczesna, Poznań 1999.
10. Piwowarski J., *Nauki o bezpieczeństwie. Kultura bezpieczeństwa i redefinicja środowiska bezpieczeństwa*, Wydawnictwo Difin, Warszawa 2020.
11. Sienkiewicz P., Nowak J.S. (red.), *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, Polskie Towarzystwo informatyczne – Oddział Górnośląski, Katowice 2008, https://delibra.bg.polsl.pl/Content/24504/BCPS_27164_2006_Spoleczenstwo-inform.pdf.
12. Szczepański A., *Pojęcie bezpieczeństwa i jego typologia – próba systematyzacji*, Zeszyty Naukowe Collegium Witelona, nr 48(3), 2023.
13. Wiejak A., *Cyberrewolucja. Nowy totalitaryzm*, Wydawnictwo AA s.c., Kraków 2025.
14. Wielka Encyklopedia PWN, Wydawnictwo Naukowe PWN, Warszawa 2003-2005.
15. Zamoyska J., *Myśli wybrane*, Fundacja Servire Veritati Instytut Edukacji Narodowej, Lublin 2013.

[57] Ibidem, s. 88.



ISBN 978-83-68103-19-9