Leszek Elak[1]
Akademia Sztuki Wojennej w Warszawie
Marek Ciekanowski[2]
Społeczna Akademia Nauk filia w Warszawie

https://doi.org/10.29316/9788368103373_3

CHARAKTERYSTYKA I UWARUNKOWANIA WSPÓŁCZESNYCH ZAGROŻEŃ BEZPIECZEŃSTWA – ASPEKTY MILITARNE, CYBERNETYCZNE I ŚRODOWISKOWE

CHARACTERISTICS AND CONTEXT OF CONTEMPORARY SECURITY THREATS – MILITARY, CYBER, AND ENVIRONMENTAL ASPECTS

Streszczenie

Współczesne środowisko bezpieczeństwa charakteryzuje się rosnącą liczbą zagrożeń o zróżnicowanym charakterze, obejmujących zarówno działania militarne i asymetryczne, jak i zagrożenia technologiczne oraz środowiskowe. Do najistotniejszych należą konflikty hybrydowe, cyberataki, terroryzm oraz katastrofy środowiskowe, które mogą destabilizować funkcjonowanie państw, wpływać na bezpieczeństwo społeczeństwa oraz zakłócać działanie infrastruktury krytycznej. Celem rozdziału jest przedstawienie istoty tych zagrożeń, ich genezy, sposobów oddziaływania oraz

[1] https://orcid.org/0000-0002-5255-9768, e-mail: l.elak@akademia.mil.pl
[2] https://orcid.org/0009-0009-1271-0652, e-mail: marek@ciekanowski.pl

znaczenia dla bezpieczeństwa państwa. Problem badawczy sformułowano: w jaki sposób konflikty hybrydowe, cyberataki, terroryzm oraz katastrofy środowiskowe oddziałują na bezpieczeństwo państwa i społeczeństwa? Przyjęto hipotezę, że współczesne zagrożenia bezpieczeństwa mają charakter złożony i wielowymiarowy, a ich skuteczne ograniczanie wymaga zintegrowanych działań państwa w sferze militarnej, organizacyjnej, technologicznej i prawnej. W opracowaniu wykorzystano metodę analizy literatury przedmiotu, analizę dokumentów i opracowań dotyczących bezpieczeństwa oraz metodę porównawczą, co pozwoliło na ukazanie omawianych zjawisk w szerszym kontekście funkcjonowania systemów bezpieczeństwa. Przeprowadzona analiza wskazuje, że współczesne zagrożenia często występują równocześnie i wzajemnie się uzupełniają, dlatego skuteczne przeciwdziałanie im wymaga kompleksowego podejścia do bezpieczeństwa, obejmującego współpracę instytucji państwowych, rozwój technologii, działania prewencyjne oraz podnoszenie świadomości społecznej.

Słowa kluczowe: bezpieczeństwo państwa, cyberataki, konflikty hybrydowe, terroryzm, katastrofy środowiskowe

Abstract

The modern security environment is characterised by a growing number of diverse threats, including both military and asymmetric operations, as well as technological and environmental threats. The most important are hybrid conflicts, cyberattacks, terrorism, and environmental disasters, which can destabilise state functioning, affect societal security, and disrupt the operation of critical infrastructure. The aim of the chapter is to present the essence of these threats, their genesis, their impact, and their significance for national security. The research problem was formulated as follows: how do hybrid conflicts, cyberattacks, terrorism, and environmental disasters affect the security of the state and society? The hypothesis was adopted that contemporary security threats are complex and multidimensional, and their effective reduction requires integrated state actions in the military, organisational, technological and legal spheres. The study uses the methods of analysing the literature on the subject, analysing documents and studies on security, and the comparative method, which allows for presenting the discussed phenomena in the broader context of the functioning of security systems. The analysis indicates that contemporary threats often occur simultaneously and complement each other, so effective countermeasures require a comprehensive security approach that includes cooperation among state institutions, technology development, preventive measures, and increased social awareness.

Keywords: state security, cyberattacks, hybrid conflicts, terrorism, environmental disasters

Wstęp

Współczesne środowisko bezpieczeństwa charakteryzuje się wysoką dynamiką zmian oraz rosnącą złożonością zagrożeń, które coraz częściej mają charakter wielowymiarowy i trudny do jednoznacznej identyfikacji. Postęp technologiczny, globalizacja, rozwój cyberprzestrzeni, a także nasilające się procesy społeczno-polityczne i środowiskowe sprawiają, że państwa muszą mierzyć się z nowymi formami oddziaływania, wykraczającymi poza tradycyjnie rozumiane konflikty zbrojne. Współczesne zagrożenia obejmują zarówno działania o charakterze militarnym i asymetrycznym, jak i zagrożenia wynikające z działalności człowieka, zmian klimatycznych czy rozwoju infrastruktury przemysłowej i teleinformatycznej. Szczególne znaczenie w tym kontekście zyskują konflikty hybrydowe, cyberataki, terroryzm oraz katastrofy środowiskowe. Zjawiska te, mimo odmiennego charakteru, łączy zdolność do destabilizowania funkcjonowania państw, zakłócania działania infrastruktury krytycznej, wywoływania strat gospodarczych oraz oddziaływania na społeczeństwo poprzez wytwarzanie poczucia zagrożenia i niepewności. W wielu przypadkach zagrożenia te występują równocześnie i wzajemnie się przenikają, co dodatkowo utrudnia skuteczne przeciwdziałanie.

Celem niniejszego rozdziału jest przedstawienie istoty oraz charakterystyki wybranych współczesnych zagrożeń dla bezpieczeństwa, ze szczególnym uwzględnieniem konfliktów hybrydowych, cyberataków, terroryzmu oraz katastrof środowiskowych. W opracowaniu omówiono genezę tych zjawisk, ich podstawowe definicje, mechanizmy oddziaływania oraz przykłady występowania, a także wskazano ich znaczenie dla bezpieczeństwa państwa i społeczeństwa.

Analiza została oparta na metodzie analizy literatury przedmiotu, materiałów źródłowych oraz dostępnych opracowań dotyczących bezpieczeństwa i zarządzania kryzysowego. Pozwoliło to na ukazanie omawianych zagrożeń w szerszym kontekście funkcjonowania współczesnych państw oraz systemów bezpieczeństwa. Podjęta problematyka ma istotne znaczenie zarówno w wymiarze teoretycznym, jak i praktycznym, gdyż właściwe rozpoznanie charakteru współczesnych zagrożeń stanowi podstawę skutecznego planowania działań zapobiegawczych, reagowania kryzysowego oraz budowania odporności państwa i społeczeństwa na sytuacje nadzwyczajne.

Istota i charakter konfliktów hybrydowych we współczesnym środowisku bezpieczeństwa

Pojęcie wojny hybrydowej zostało rozpowszechnione pierwszy raz przez Franka Hoffmana jako „jakikolwiek adwersarz używający kombinacji broni konwencjonalnej, nieregularnej taktyki, terroryzmu i przestępczości w tym samym czasie i na tym samym polu bitwy celem osiągnięcia celów politycznych" (Hajduk, Stępniewski, 2015). Pomimo tego, początki tej idei sięgają lat 60. XX wieku. Za pierwszego autora opisującego konflikty, które współcześnie określamy mianem wojen hybrydowych, uznaje się Jewgienija Messnera – twórcę koncepcji wojny buntowniczej. W swoich analizach Messner podkreślał, że nowoczesna wojna może przyjmować charakter ograniczony koalicyjnie lub mieć wymiar światowy. Ilustrował to na przykładzie wojny koreańskiej, podczas której Chiny jawnie wspierały Koreę Północną, natomiast Związek Radziecki angażował się nieoficjalnie. Zdaniem Messnera powodowało to zmianę przeciwnika, tradycyjnie rozumianego jako siły zbrojne wrogiego państwa. Od teraz uważał on, że głównym przeciwnikiem w wojnie będzie cały naród, a cały naród może być atakowany nie tylko środkami kinetycznymi, które to są dosyć kosztowne dla państw. W konfliktach określanych jako wojny buntownicze obserwuje się zacieranie granicy pomiędzy działaniami zbrojnymi uznawanymi przez prawo międzynarodowe za legalne a metodami walki zakwalifikowanymi jako bezprawne. Wynika to z braku wyraźnego rozgraniczenia między siłami zbrojnymi a ludnością cywilną. W tego rodzaju konfliktach kluczową rolę odgrywają formacje nieregularne, powoływane przez niezadowolone grupy społeczne, takie jak uzbrojeni członkowie organizacji zawodowych, którzy w warunkach miejskich mogą stanowić istotny czynnik siły. Zatarcie granic pomiędzy armią regularną a nieregularną prowadzi jednocześnie do erozji zasad etyki wojennej. Messner zwracał uwagę, że zmieniający się charakter wojny wymusza na sztabach skupienie się na rozwijaniu strategii, działań operacyjnych oraz taktyki opartej na terrorze, podstępie i zdradzie (Hajduk, Stępniewski, 2015).

Dalszy rozwój technologiczny, rewolucja cyfrowa i wprowadzenie nowych środków przekazu (mass media pokroju telewizji czy radia, ale także socialmediów) doprowadziły do sytuacji, w której działania hybrydowe bardzo mocno skupiają się na informacjach kierowanych do społeczeństwa

(Kamionka, 2023, s. 62). Już Messner w swoim dziele pisał o potrzebie działania informacyjnego na nieprzyjacielu, którą określał mianem *dywersji informacyjnej* (obok klasycznych dywersji i sabotażu). Do tego szczególnie ważne staje się dokładne zidentyfikowanie sposobów funkcjonowania systemów wczesnego ostrzegania przeciwnika oraz jego procedur zarządzania kryzysowego. Poza analizą kondycji systemu finansowego państwa i jego zdolności obronnych, kluczowe znaczenie ma również zgromadzenie pogłębionych danych dotyczących obiektów i sieci o znaczeniu strategicznym. Do najistotniejszych należą tu rozwiązania z zakresu teleinformatyki, infrastruktura transportowa, systemy produkcji i dystrybucji energii, w tym sieci gazowe, naftowe i elektroenergetyczne, dostępność zasobów surowcowych i paliwowych, a także mechanizmy zapewniające ciągłość dostaw żywności i wody oraz sprawne funkcjonowanie opieki zdrowotnej (Sykulski, 2015, s. 106-107).

Z perspektywy podmiotów planujących działania polityczno-militarne zgodnie z założeniami koncepcji J. Messnera kluczowe znaczenie ma stopniowe doprowadzenie do narastania frustracji wśród szerokich warstw społeczeństwa oraz pogłębianie sporów w obrębie elit władzy. Następnie dąży się do osłabienia sytuacji gospodarczej, inicjowania niepokojów społecznych, a w konsekwencji do eskalacji w postaci jawnych działań zbrojnych. Są one prowadzone między innymi przez odpowiednio przygotowane jednostki sił specjalnych oraz funkcjonariuszy służb specjalnych, którzy działają po stronie przeciwnika. Skuteczność wojny buntowniczej w znacznym stopniu zależy od efektywnego prowadzenia operacji informacyjnych, obejmujących zarówno oddziaływanie na społeczeństwo państwa będącego celem ataku, jak i wpływanie na opinię międzynarodową. Istotnym elementem tych działań jest podważanie wiarygodności i reputacji atakowanego państwa, co w optymalnym wariancie prowadzi do jego politycznej izolacji. Realizacja koncepcji Messnera zakłada przede wszystkim unikanie oficjalnego udziału państwa w otwartym konflikcie zbrojnym. Grupy dywersyjne zaangażowane w działania nie posiadają oznaczeń identyfikujących ich przynależność, a ich uczestnicy – w świetle prawa międzynarodowego – nie są uznawani za żołnierzy regularnych sił zbrojnych. Pozwala to państwu inicjującemu na formalne zaprzeczenie swojemu zaangażowaniu w przypadku silnego oporu ze strony przeciwnika. W rezultacie dochodzi do swoistego

„odpaństwowienia" zarówno formacji zbrojnych, jak i samego konfliktu, który z zewnętrznej perspektywy może być postrzegany jako wojna domowa lub przejaw wewnętrznego chaosu.

W konfliktach określanych jako wojny buntownicze nie funkcjonuje tradycyjna linia frontu, a działania mogą zostać zapoczątkowane wewnątrz państwa, często z dala od jego granic. Istotnym elementem jest wykorzystywanie skupisk mniejszości narodowych i etnicznych, które mogą stanowić podatny grunt do wywoływania napięć społecznych i zamieszek, a jednocześnie pełnić rolę zaplecza logistycznego dla prowadzonych operacji. Ważnym aspektem przygotowań do tego typu konfliktów jest również inspirowanie oraz finansowe wspieranie ugrupowań radykalnych i ekstremistycznych, zarówno politycznych, jak i religijnych, działających na terytorium państw uznawanych za wrogie, a następnie rozwijanie ich aktywności w oparciu o strategię oporu niekierowanego (Sykulski, 2015). Z tego względu kluczowe znaczenie ma sprawne wykorzystanie zdolności wywiadowczych oraz skuteczne prowadzenie walki informacyjnej, która umożliwia przeniesienie konfrontacji z klasycznego pola walki do znacznie szerszej przestrzeni oddziaływania. Obejmuje ona przede wszystkim sferę świadomości społecznej, określaną jako noosfera, a także cyberprzestrzeń. Decydującą rolę odgrywają tu długofalowe działania psychologiczne i informacyjne, nastawione na stopniowe kształtowanie postaw, emocji i przekonań społeczeństwa.

Rozwojowi wojen buntowniczych sprzyja ponadto powstawanie niewielkich i słabych państw oraz wzrost znaczenia podmiotów nieuznawanych i dysfunkcyjnych, określanych mianem państw upadłych. Jewgienij Messner już na początku lat siedemdziesiątych XX wieku wskazywał na rosnącą rolę terroru jako narzędzia walki, w tym możliwość zastosowania skrajnych środków oddziaływania, takich jak punktowe użycie taktycznych ładunków jądrowych czy tzw. brudnych bomb, których głównym celem byłoby wywołanie silnego efektu psychologicznego. W tego rodzaju działaniach szczególnie istotne pozostają morale społeczeństwa oraz zdolność aparatu państwowego do opanowania narastającego strachu w taki sposób, aby nie przerodził się on w powszechną panikę. Już w okresie międzywojennym w działalności Kremla można dostrzec świadome stosowanie elementów strategii, które dziś określamy mianem wojny hybrydowej. ZSRR, formalnie pozostając w stanie pokoju z Polską po traktacie ryskim z 1921 roku, nie rezygnował z dążenia

do osłabienia sąsiedniego państwa przez działania poniżej oficjalnego progu otwartego konfliktu zbrojnego. Na północno-wschodnich rubieżach II RP, szczególnie na terenach Kresów zamieszkałych przez mniejszości narodowe, częste były prowokacje i akcje dywersyjne, które miały destabilizować sytuację społeczno-polityczną i podważać autorytet władz polskich.

Strategia ta zaczęła się ujawniać już w pierwszej połowie lat 20. XX wieku, choć najbardziej intensywnie realizowana była w 1924 r. Sowiecka agencja wywiadu wojskowego, Razwiedupr, kierowana przez zaawansowanych oficerów takich jak Jan Berzin, prowadziła zorganizowane działania dywersyjne na obszarach województw wileńskiego, nowogródzkiego i poleskiego. Celem było nie tylko sianie niepokoju, ale także przygotowanie warunków do ewentualnego powstania, które mogłoby posłużyć do ewentualnej aneksji tych terenów do ZSRR (Rodak, 2016). W praktyce działania te przybierały formę regularnych ataków na instytucje państwowe i strategiczne punkty II RP. Jednym z najbardziej znanych incydentów był atak na Stołpce w nocy z 3 na 4 sierpnia 1924 r., kiedy to około sześćdziesięcioosobowy oddział, prawdopodobnie dowodzony przez oficera sowieckiego wywiadu Stanisława Waupszasowa, przeprowadził skoordynowany atak na starostwo, posterunki policji i koszary, zabijając policjantów i cywilów oraz doprowadzając do chaosu w mieście tuż przy polsko-sowieckiej granicy (Rodak, 2016).

Podstawą sukcesów tych operacji była nie tylko agresja militarna w formie partyzanckiej, ale też wielostronna działalność propagandowa i agitacyjna wśród miejscowej ludności, szczególnie Białorusinów i Ukraińców, którzy często byli niezadowoleni z sytuacji społeczno-gospodarczej po I wojnie światowej i traktach powojennych. Sowieccy agitatorzy, często wracający repatrianci lub weterani Armii Czerwonej, potrafili wykorzystać lokalne niezadowolenie i historyczne antagonizmy, by zwiększać podatność ludności na idee komunistyczne i antypaństwowe.

Aktywność dywersyjna była na tyle nasilona, że w 1924 r. odnotowano co najmniej 207 incydentów zbrojnych tego typu na Kresach, co świadczy o skoordynowanym i długotrwałym charakterze tej ofensywy. Oddziały Razwiedupru korzystały zarówno z własnych ludzi, jak i lokalnych rekrutów, w tym działaczy Komunistycznej Partii Zachodniej Białorusi czy elementów przestępczych.

Dopiero zdecydowane środki podjęte przez polski rząd w postaci utworzenia Korpusu Ochrony Pogranicza oraz represji wobec działaczy proradzieckich doprowadziły do spadku liczby incydentów w regionie w 1925 r. Sowiecka operacja hybrydowa została częściowo wygaszona również z powodu zmian wewnętrznych w Moskwie i rosnącej krytyki wewnątrz sowieckich struktur wywiadowczych, co doprowadziło do oficjalnego zaniechania akcji (Rodak, 2016).

W 2014 roku Rosja prowadziła wobec Ukrainy działania o charakterze wojny hybrydowej, łącząc środki militarne, informacyjne i polityczne w sposób mający na celu osiągnięcie strategicznych celów bez formalnego wypowiedzenia wojny (Elak i in., 2024). Konflikt rozpoczął się od wydarzeń wokół Krymu, gdzie w lutym rosyjskie siły specjalne, pozbawione oficjalnych oznaczeń, zajęły budynki rządowe i przejęły kontrolę nad półwyspem (Oskierko i in., 2025). Te nieoznakowane jednostki, określane później mianem „zielonych ludzików", stanowiły przykład zastosowania sił zbrojnych w sposób zamaskowany, co utrudniało przypisanie im jednoznacznej odpowiedzialności państwowej. Zajęcie Krymu zakończyło się formalną aneksją półwyspu przez Rosję w marcu 2014 roku, mimo że nie doszło do oficjalnej wojny między państwami (Instytut Nowej Europy, b.d.).

Równocześnie Rosja prowadziła operacje informacyjne i propagandowe, które miały podważać legitymację władz w Kijowie po wydarzeniach Euromajdanu oraz tworzyć narracje uzasadniające ingerencję w sprawy Ukrainy, w tym ochronę ludności rosyjskojęzycznej. Prowadzono dezinformację zarówno wewnątrz Ukrainy, jak i wobec opinii międzynarodowej, co miało na celu stworzenie wewnętrznych podziałów społecznych i osłabienie odporności państwa ukraińskiego (Kłaczyński, 2019). Agresja Rosji na Ukrainę pokazała słabą jedność Europy wobec zagrożeń zewnętrznych, wynikającą z rozbieżnych interesów państw UE. Wydarzenia takie jak Euromajdan i wojna hybrydowa nie doprowadziły do wspólnego stanowiska w sprawach wschodnich (Trofymowych, 2016, s. 184).

Unia Europejska powinna wypracować spójną strategię wobec zagrożeń hybrydowych, wzmacniać zdolności analityczne i operacyjne oraz zwiększać samodzielność w zakresie bezpieczeństwa. Ważne jest też rozwijanie współpracy z NATO i innymi partnerami oraz zwalczanie szantażu migracyjnego (Żurawski, Oskierko, 2025, s. 65).

Zagrożenia środowiskowe i ich wpływ na bezpieczeństwo państwa

Na początku warto rozróżnić katastrofę środowiskową i ekologiczną. Katastrofa ekologiczna oznacza nieodwracalne zniszczenie uniemożliwiające przetrwanie gatunków, natomiast środowiskowa obejmuje każde katastrofalne zdarzenie w środowisku. W referacie autor skupi się na katastrofach środowiskowych ze względu na ich precyzyjne znaczenie. Katastrofa ekologiczna to trwałe zaburzenie struktur i funkcji ekosystemu bez możliwości kompensacji. Katastrofa ekologiczna skutkuje nieodwracalnymi zmianami jakościowymi i ilościowymi w łańcuchach troficznych. Rozróżnia się katastrofy ekologiczne antropogeniczne – powodowane przez człowieka, i nieantropogeniczne, zwane też katastrofami naturalnymi, wywoływane przez czynniki niezależne od człowieka. Do powodowanych przez czynniki ludzkie możemy zaliczyć:

- długotrwałe emisje szkodliwych substancji,
- zanieczyszczanie mórz i oceanów np. w wyniku wycieku ropy z tankowca,
- awarie przemysłowe powodujące wycieki substancji radioaktywnych i toksycznych.

Zaś do katastrof naturalnych (nieantropogenicznych) należą:

- huragany, tornada fale zimna bądź upałów, powodzie, susze,
- tsunami, wybuchy wulkanów, trzęsienia ziemi,
- pożary lasów, osuwiska i lawiny.

Czynniki antropogeniczne, oddziałując łącznie z procesami naturalnymi, często prowadzą do katastrof ekologicznych, których konsekwencje obejmują rozległe obszary lub mają zasięg globalny. Przykładowo, intensywna, monokulturowa gospodarka rolna w połączeniu z niekorzystnymi warunkami klimatycznymi sprzyja pustynnieniu znacznych terenów Ziemi, natomiast emisja dwutlenku węgla oraz innych gazów cieplarnianych, współdziałając z parą wodną obecną w atmosferze, potęguje efekt cieplarniany, co może skutkować istotnym wzrostem poziomu oceanów na skutek topnienia lodowców. Trzęsienia ziemi to jedne z najbardziej niebezpiecznych klęsk żywiołowych. Powstają wskutek nagłego uwolnienia energii w skorupie ziemskiej, najczęściej przez procesy tektoniczne. Silne wstrząsy (powyżej 6

stopni w skali Richtera) mogą powodować rozległe zniszczenia budynków, infrastruktury oraz poważne straty ludzkie.

Na terenach górskich wstrząsy sejsmiczne mogą wywoływać osuwiska i lawiny, natomiast trzęsienia podmorskie prowadzą do powstawania potężnych fal tsunami. Dane średnioroczne wskazują, że na świecie występuje około 100 trzęsień ziemi o magnitudzie powyżej 6 stopni w skali Richtera, co oznacza, że zjawisko to pojawia się średnio co kilka dni. Statystyki z lat 1984-1994 ukazują skalę jego tragicznych konsekwencji – około 90 tysięcy ofiar śmiertelnych, blisko pół miliona rannych oraz kilka milionów osób pozbawionych dachu nad głową. Należy również zaznaczyć, że trzęsienia ziemi mogą mieć charakter wzbudzony, np. w wyniku eksplozji jądrowych przeprowadzanych na obszarach aktywnych sejsmicznie.

Pożar definiuje się jako niekontrolowane i samorzutne rozprzestrzenianie się ognia, które stanowi bezpośrednie zagrożenie dla życia i zdrowia ludzi oraz powoduje poważne straty materialne. Współcześnie zjawisko to należy do jednych z istotniejszych zagrożeń o charakterze naturalnym i cywilizacyjnym. Pożary o podłożu naturalnym mogą być wywoływane przez różnorodne czynniki, takie jak wyładowania atmosferyczne, procesy samozapłonu (np. torfu czy siana), skupienie promieni słonecznych przez szkło lub soczewki, a także uszkodzenia infrastruktury energetycznej. Szczególnie dotkliwe konsekwencje środowiskowe niosą ze sobą pożary lasów i obszarów puszczańskich. Zjawiska te prowadzą do znacznej emisji gazów cieplarnianych, nasilają procesy erozji gleb, a także powodują lokalne zmiany warunków klimatycznych i hydrologicznych. Pożary niszczą nie tylko rozległe obszary drzewostanu, generując istotne straty ekonomiczne, lecz również leśne zasoby użytkowe oraz uprawy. W ich wyniku obniżeniu ulegają kluczowe funkcje lasu, takie jak zdolność retencjonowania wody czy jego korzystny wpływ na stan środowiska przyrodniczego. Ponadto dochodzi do degradacji cennej fauny oraz zakłócenia planowej gospodarki leśnej. Pożary obejmujące duże obszary stanowią również bezpośrednie zagrożenie dla pobliskich miejscowości i osiedli ludzkich.

Następnym zjawiskiem są burze i huragany. Gdy prędkość wiatru jest odpowiednio wysoka, skutki takich czynników mogą spowodować katastrofalne w skutkach zniszczenia budynków i urządzeń, a także śmierci ludzi i zwierząt. Huragany i trąby powietrzne sieją na swej drodze spustoszenia na

lądzie. Sztorm wywołuje wysokie i silne fale na morzu, które stanowią zagrożenie dla jednostek pływających i platform wiertniczych, a wdzierając się na brzeg, powodują przybrzeżne powodzie i wiele zniszczeń urządzeń brzegowych. Częstym zjawiskiem towarzyszącym są wybuchy przemysłowe. W ich wyniku dochodzi do zniszczenia obiektów i instalacji technicznych, powstawania pożarów oraz uszkodzeń systemów produkcyjnych. Najczęściej obserwuje się eksplozje kotłów wysokoprężnych, a także wybuchy gazów, par benzyny i innych substancji wykorzystywanych w przemyśle naftowym. Do najbardziej tragicznych w skutkach należą jednak eksplozje pyłu węglowego i gazów w kopalniach, jak również wybuchy butli gazowych oraz gazu w sieciach komunalnych. Poważne awarie przemysłowe zaliczane są do zdarzeń o charakterze nadzwyczajnym, powodujących znaczące straty w sferze zdrowotnej, środowiskowej oraz materialnej. W ich następstwie dochodzi do uwolnienia znacznych ilości substancji niebezpiecznych, które mogą oddziaływać szkodliwie na rozległe obszary. Mianem obszaru skażonego określa się teren wraz z znajdującą się na nim infrastrukturą, który został objęty działaniem substancji chemicznych, promieniotwórczych lub biologicznych. Natomiast rejon porażenia to obszar, na którym występują bezpośrednie skutki skażenia, takie jak negatywne oddziaływanie na ludzi, zwierzęta i rośliny, a także uszkodzenia sprzętu oraz różnego rodzaju obiektów spowodowane działaniem toksycznych czynników. Najważniejsza rzeczą wartą zapamiętania jest to, że rozprzestrzenianie się toksycznych środków przemysłowych stwarza zagrożenie dla życia organizmów żywych oraz wprowadza gwałtowne zmiany w naturalnym ekosystemie natury.

Katastrofy środowiskowe nasiliły się głównie przez działalność człowieka ze względu na rozwój przemysłu. Z tego względu w dzisiejszych czasach coraz bardziej rośnie znaczenie i wartość środowiska naturalnego, a samo rozumienie bezpieczeństwa ekologicznego ulega znacznej zmianie. Klęski żywiołowe, katastrofy wywołane działalnością człowieka, mogą i stanowią poważne zagrożenia dla państwa. W tej części autor postara się przedstawić działania człowieka, które mają na celu niwelowanie katastrof środowiskowych. Najważniejszym dokumentem dotyczącym bezpieczeństwa ekologicznego w Polsce jest Konstytucja RP. W rozdziale 5 podkreśla ona, że państwo zapewnia ochronę środowiska, opierając się na zasadzie zrównoważonego rozwoju. Konstytucja nakłada także obowiązek budowania

świadomości ekologicznej oraz zachęca do poszukiwania nowych dróg rozwoju z poszanowaniem środowiska. Warto tutaj wspomnieć o idei ekorozwoju, która została przedstawiona po raz pierwszy w 1975 roku przez Program Środowiskowy ONZ. Według Encyklopedii PWN, ekorozwój to długotrwały, samopodtrzymujący się rozwój gospodarczy, prowadzony z uwzględnieniem ochrony środowiska i troski o sprawiedliwość międzypokoleniową.

Podstawowe założenia światowej polityki ekorozwoju określono w 1993 roku w Deklaracji w sprawie Środowiska i Rozwoju oraz w Agendzie 21 podczas konferencji ONZ w Rio de Janeiro. Zasady ochrony środowiska, które obowiązują w polskim prawie, mają duże znaczenie: pomagają interpretować przepisy szczegółowe, wskazują kierunki przyszłych regulacji i precyzują zasady tworzenia aktów wykonawczych. Jedną z najważniejszych jest zasada zrównoważonego rozwoju, sformułowana w Deklaracji z Rio, a następnie włączona do prawa polskiego, między innymi przez art. 5 Konstytucji RP. Ustawa Prawo ochrony środowiska definiuje ją jako rozwój społeczno-gospodarczy polegający na łączeniu działań politycznych, ekonomicznych i społecznych przy jednoczesnym utrzymaniu równowagi przyrody oraz trwałości potrzeb obecnych i przyszłych pokoleń.

Zasada przezorności nakazuje podejmowanie działań zapobiegawczych, gdy brak jasnych dowodów na brak szkodliwości dla środowiska. Zasada prewencji wymaga analizy możliwych skutków przed rozpoczęciem działań, co stanowi podstawę przeciwdziałania degradacji środowiska, szczególnie poprzez procedurę oceny oddziaływania na środowisko. Obie zasady są obecne w prawie Unii Europejskiej oraz polskim systemie prawnym.

Cyberprzestrzeń jako domena zagrożeń bezpieczeństwa

Cyberatak to najnowsze zjawisko spośród tych omówionych w pracy. Wynika to z faktu, że cybernetyczne środowisko istnieje znacznie krócej niż tradycyjne zagrożenia, takie jak terroryzm, zagrożenia środowiskowe czy wojny hybrydowe, które towarzyszą ludzkości od starożytności pod różnymi nazwami i w różnych formach (Ciekanowski i in., 2023). Cyberprzestrzeń, czyli środowisko, gdzie zachodzą te ataki, powstała dopiero w latach 60. XX wieku. Pierwsze systemy cyberprzestrzeni zostały stworzone na potrzeby wojska, by umożliwić przesyłanie informacji na duże odległości między komputerami. Bodźcem do rozwoju tej technologii były ograniczenia

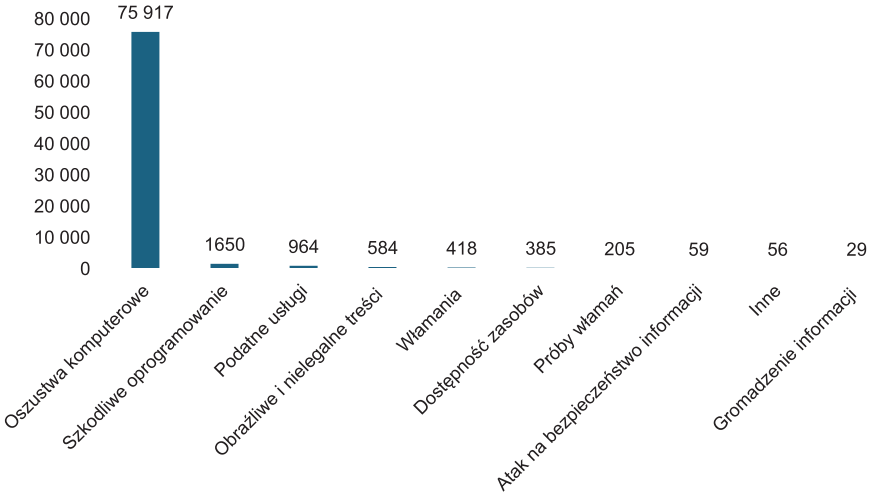
istniejących systemów komunikacji, które pozwalały na swobodną wymianę danych tylko w zamkniętych sieciach lokalnych.

Zjawisko cyberataku po dziś dzień rozwinęło się na tyle, że zostało zdefiniowane jako jedno z głównych zagrożeń i narzędzi w prowadzeniu operacji wojskowych czy pozyskiwania informacji wywiadowczych nie tylko na potrzeby państw, ale i podmiotów prywatnych. Według definicji zjawisko to oznacza każdy rodzaj ofensywnego działania w Internecie osób lub organizacji, którego celem mogą być systemy informatyczne, sieci komputerowe, komputery lub inne urządzenia osobiste (Słownik PWN, b.d.). Wartą uwagi jest również definicja podawana przez firmę Microsoft, przodującą w produkcji oprogramowania komputerowego. Definicja mówi natomiast o cyberataku jako celowe działanie osoby lub grupy osób mające na celu naruszenie, uszkodzenie lub zakłócenie działania systemów komputerowych, sieci lub urządzeń cyfrowych, często w złych zamiarach, takich jak kradzież danych, szpiegostwo, oszustwa finansowe lub sabotaż systemu (Microsoft, b.d.).

Wymienione w definicjach obiekty narażone na cyberataki i ich cele są skrupulatnie realizowane przez przeciwników nie tylko biznesowych czy przestępczych, ale w szczególności państwowych. Do zrealizowania takich celów ataków jak zawartych w definicji podmioty agresorów cyberprzestrzeni wykorzystują metody takie jak:

- Ataki malware,
- Phishing i sphere phishing,
- DoS, DDoS,
- MitM,
- Ransomware.

Poniżej na Rysunku 1 przedstawiono incydenty obsłużone przez CERT Polska w 2023 r. w podziale na kategorie.



Rysunek 1. Incydenty obsłużone przez CERT Polska w 2023 r. w podziale na kategorie

Źródło: CERT, 2023.

Powyższe metody ataków są najpopularniejszymi i najchętniej wykorzystywanymi ze względu na ich metodę przebiegu. Przykładowo, ataki malware polegają na uzyskaniu nieuprawnionego dostępu do określonego urządzenia czy sieci za pomocą szkodliwego oprogramowania lub nieświadomego dawania dostępu nieupoważnionej osobie (Trend Micro, b.d.).

W ujęciu Państwa polskiego cyberataki zyskują na znaczeniu w kwestii bezpieczeństwa tak samo jak w środowisku prywatnym i biznesowym. Cyberataki zyskują na znaczeniu w kwestii bezpieczeństwa tak samo jak w środowisku prywatnym i biznesowym, co zyskuje dodatkowe znaczenie na przestrzeni ostatnich lat, odkąd Rosja zintensyfikowała działania pod progiem wojny na nasz kraj. Jak pokazują statystyki, w Polsce dochodzi do 1500 cyberataków tygodniowo, co jest wzrostem w porównaniu z rokiem 2024 o 23% (Pasławski, 2025).

W związku z takimi wzrostami zagrożenia cyberatakami na podmioty naszego państwa, które trwają od ponad dekady, władze systematycznie rozwijają zdolności kontrdziałania przeciwko temu zjawisku.

Począwszy od napisania Doktryny Cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 roku. Doktryna ta zawiera elementy zdefiniowania poszczególnych zjawisk zachodzących w sferze cyberbezpieczeństwa oraz

cele, jak i środki przeciwdziałania tym zagrożeniom. W toku ewolucji świadomości państwa do zapobiegania tym aktom agresji siły zbrojne również dostrzegły potencjał domeny cyber do oddziaływania na przeciwnika oraz zdobywania przewagi informacyjnej. Doprowadziło to w roku 2022 do sformowania Wojsk Obrony Cyberprzestrzeni jak i ich odpowiednika w strukturze Wojsk Obrony Terytorialnej. Przez zdobycie takich elementów państwo uzyskało zdolności do kontrowania przyszłych zagrożeń, jakie stoją przed państwem. Jednakże w odróżnieniu od wojsk konwencjonalnych wojska cybernetyczne nie są ograniczone swoim terenem i mogą oddziaływać w czasie rzeczywistym w dowolnym miejscu na świecie, co, jak pokazują przykłady z historii, jest ich największym atutem w świecie zinformatyzowanych instytucji i nowoczesnych armii.

Takie formacje, zarówno nasze, jak i przeciwnika, mogą również rozmywać swoją odpowiedzialność za pomocą aktorów pozapaństwowych, jak robi to Federacja Rosyjska za pomocą tak zwanych farm trolli, czy Chiny przez PLA 61389, które w ramach swoich działań nie posiadają bezpośrednich jawnych powiązań ze strukturami swojego państwa, a niejednokrotnie swoje operacje wykonują z terenów nie należących do państwa, pod które podlegają. Ich operacje również nie stanowią jawnej operacji wojskowej, a jedynie wykupienie usługi u grup hakerskich lub stworzenie fikcyjnej grupy hakerskiej, tak jak ma to miejsce w przypadku chińskim (Volt Typhoon, APT31 i APT41) (Makeittogether, b.d.).

Taki sposób zarządzania siłą w cyberprzestrzeni prowadzi do sytuacji, w których sprawca cyberataku nie może zostać zidentyfikowany na bieżąco, a jedynie po długotrwałym dochodzeniu. Uniemożliwia to szybką i adekwatną reakcję podczas trwania ataku. Ten problem przestaje mieć znaczenie jedynie w sytuacjach otwartej agresji zbrojnej, kiedy działania w cyberprzestrzeni stanowią wsparcie tradycyjnych operacji militarnych.

Podsumowanie

Przeprowadzona analiza wskazuje, że współczesne środowisko bezpieczeństwa charakteryzuje się dużą dynamiką zmian oraz rosnącą złożonością zagrożeń, które coraz częściej mają charakter wielowymiarowy i wzajemnie powiązany. Konflikty hybrydowe, cyberataki, terroryzm oraz katastrofy środowiskowe stanowią istotne wyzwania dla funkcjonowania państw,

ponieważ oddziałują nie tylko na sferę militarną, lecz także na gospodarkę, infrastrukturę krytyczną, środowisko naturalne oraz bezpieczeństwo społeczne. Szczególnie istotnym zjawiskiem jest zacieranie się granic pomiędzy stanem pokoju i konfliktem, co utrudnia jednoznaczne rozpoznanie zagrożeń oraz podjęcie adekwatnych działań zapobiegawczych i reagowania.

Współczesne zagrożenia cechują się również wysokim stopniem nieprzewidywalności oraz możliwością występowania efektów kaskadowych, w których jedno zdarzenie może prowadzić do kolejnych kryzysów w innych obszarach funkcjonowania państwa. Rozwój technologii informatycznych i telekomunikacyjnych, globalizacja oraz postępujące zmiany środowiskowe powodują, że państwa są coraz bardziej podatne na różnego rodzaju oddziaływania, zarówno ze strony innych państw, jak i podmiotów niepaństwowych.

Wnioskiem wynikającym z przeprowadzonych rozważań jest konieczność stosowania kompleksowego i zintegrowanego podejścia do bezpieczeństwa, obejmującego działania prewencyjne, rozwój systemów wczesnego ostrzegania, wzmacnianie odporności infrastruktury krytycznej, a także podnoszenie poziomu świadomości społecznej. Kluczowe znaczenie ma również współpraca międzynarodowa oraz stałe doskonalenie systemów zarządzania kryzysowego, które umożliwiają skuteczne reagowanie na pojawiające się zagrożenia.

Współczesne państwa, aby skutecznie przeciwdziałać nowym formom zagrożeń, powinny rozwijać zarówno zdolności technologiczne i organizacyjne, jak i mechanizmy prawne oraz instytucjonalne, pozwalające na szybkie i adekwatne reagowanie na sytuacje kryzysowe. Tylko takie podejście umożliwia ograniczanie skutków zagrożeń oraz zapewnienie stabilnego i bezpiecznego funkcjonowania państwa i społeczeństwa.

Literatura

1. CERT. (2023). *Raport roczny z działalności CERT Polska*. Pobrane z: https://cert.pl/posts/2024/04/raport-roczny-2023 (dostęp: 17.01.2026).
2. Ciekanowski, Z., Gruchelski, M., Nowicka, J., Żurawski, S., Pauliuchuk, Y. (2023). Cyberspace as a source of new threats to the security of the European Union. *European Research Studies Journal, 26*(3), 782-797.

3. Elak, L., Oskierko, M., Żurawski, S. (2024). Ochrona granicy polsko-białoruskiej w obliczu wojny hybrydowej. *De Securitate et Defensione. O Bezpieczeństwie i Obronności, 10*(1), 81-95.
4. Hajduk, J., Stępniewski, T. (2015). Wojna hybrydowa Rosji z Ukrainą: Uwarunkowania i instrumenty. *Studia Europejskie, 4,* 135-152.
5. Instytut Nowej Europy. (b.d). Wszystko *jest wojną. Rosyjskie działania hybrydowe wobec państw Trójmorza*. Pobrane z: https://ine.org.pl/wszystko-jest-wojna-rosyjskie-dzialania-hybrydowe-wobec-panstw-trojmorza (dostęp: 17.01.2026).
6. Kamionka, M. (2023). Rosyjska wojna hybrydowa w mediach społecznościowych na przykładzie portalu Facebook. *Wiedza Obronna*, *82*(1), 63-76.
7. Kłaczyński, R. (2019). Rosyjsko-ukraiński konflikt 2014-2017 jako przykład wojny hybrydowej. Geneza, Polityka, Gospodarka. *Rocznik Bezpieczeństwa Międzynarodowego, 11*(2), 78-90.
8. Microsoft. (b.d.). *Co to jest cyberatak?* Pobrane z: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-a-cyberattack (dostęp: 17.01.2026).
9. Makeittogether. (b.d.). *Raport Sophos: Chińskie grupy hakerskie eskalują, ataki na urządzenia brzegowe*. Pobrane z: https://makeittogether.pl/raport-sophos-chinskie-grupy-hakerskie-eskaluja-ataki-na-urzadzenia-brzegowe (dostęp: 17.01.2026).
10. Oskierko, M., Nasiadka, A., Ochyra-Żurawska, K. (2025). Wojska Obrony Terytorialnej w ochronie granicy państwowej w warunkach wojny hybrydowej. *Prawo i Bezpieczeństwo, 2*(5), 98-110.
11. Pasławski, K., CRN. (b.d.). *Ponad 1800 cyberataków tygodniowo na polskie firmy.* Pobrane z: https://crn.pl/aktualnosci/ponad-1800-atakow-tygodniowo-na-polskie-firmy/ (dostęp: 17.01.2026).
12. Rodak, W. (2016). *Leśna, Łowcza i Stołpce. Wojna hybrydowa na kresach II RP. Zielone ludziki 1.0*. Pobrane z: https://naszahistoria.pl/lesna-lowcza-i-stolpce-wojna-hybrydowa-na-kresach-ii-rp-sowieckie-zielone-ludziki-10/ar/c1-9813528#google_vignette (dostęp: 17.01.2026).
13. Sykulski, L. (2015). Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera. *Przegląd Geopolityczny, 11,* 103-112.

14. Słownik PWN. (b.d.). *Cyberatak*. Wydawnictwo Naukowe PWN. Pobrane z: https://sjp.pwn.pl/sjp/cyberatak,5606168.html#google_vignette (dostęp: 17.01.2026).
15. Trendmicro. (b.d.). *15 najczęstrzych rodzajów cyberataków*. Pobrane z: https://www.trendmicro.com/pl_pl/what-is/cyber-attack/types-of-cyber-attacks.html (dostęp: 17.01.2026).
16. Trofymowych, V. (2016). Wojna hybrydowa jako instrument kluczowy rosyjskiej geostrategii rewanżu. *Ante Portas – Studia nad Bezpieczeństwem*, *1*(6), 175-186.
17. Żurawski, S., Oskierko, M. (2025). Unia Europejska wobec kryzysu migracyjnego jako narzędzia wojny hybrydowej. *De Securitate Et Defensione. O Bezpieczeństwie i Obronności*, *11*(1), 51-67.