Asymetryczność konfliktów w XXI wieku

redakcja naukowa
Izabela OLEKSIEWICZ

OFICYNA
WYDAWNICZA
POLITECHNIKI RZESZOWSKIEJ

Wydano za zgodą Rektora

R e c e n z e n t
dr hab. Marta POMYKAŁA, prof. PRz

R e d a k t o r n a c z e l n y
Wydawnictw Politechniki Rzeszowskiej
dr hab. inż. Lesław GNIEWEK, prof. PRz

R e d a k t o r
Piotr CYREK

S k ł a d i ł a m a n i e
Mariusz TENDERA

P r o j e k t o k ł a d k i
Anna PIECZONKA
Ilustracja wygenerowana przy użyciu AI

konflikt, państwo, asymetryczność, cyberatak, wielowymiarowość
conflict, state, asymmetry, cyberattack, multidimensionality

p-ISBN 978-83-7934-847-3 e-ISBN 978-83-7934-852-7

Oficyna Wydawnicza Politechniki Rzeszowskiej
al. Powstańców Warszawy 12, 35-029 Rzeszów
https://oficyna.prz.edu.pl

Ark. wyd. 8,41. Ark. druk. 7,75.
Wydrukowano w czerwcu 2026 r.
Drukarnia Oficyny Wydawniczej,
al. Powstańców Warszawy 12, 35-029 Rzeszów
Zam. nr 25/26

SPIS TREŚCI

WSTĘP

Relacje między wojną a pokojem jako kategoriami, których znaczenie od zawsze ewoluowało, kształtuje świat na przestrzeni dziejów. Pozostają one w ścisłym związku z rozwojem myśli politycznej, prawnej i filozoficznej. Analiza tekstów źródłowych wskazuje jednak na zdecydowanie większe zainteresowanie licznych myślicieli wojną niż pokojem. Pokój nie był zatem ściśle skorelowany z zagadnieniem wojny. Inaczej rzecz ujmując – problematyka wojny kształtowała się niezależnie do idei pokoju.

Warto zauważyć, że w starożytnej Grecji pokój był analizowany w kontekście ustroju państwa, etyki i cnót obywatelskich, a także jako sprawdzian organizacji i przywództwa. W Rzymie dominowało podejście pragmatyczne, traktujące wojnę jako narzędzie realizacji interesów państwa, oparte na dyscyplinie i efektywnej organizacji. Średniowiecze wprowadziło normatywne ograniczenia konfliktu, podporządkowując go kryteriom moralnym i prawnym oraz tworząc jeszcze koncepcję tzw. wojny sprawiedliwej. Jest to pojęcie, które od wieków wywołuje spór pomiędzy filozofami, prawnikami, politologami i teologami. W okresie nowożytnym akcent przesunął się w stronę racjonalizacji działań wojennych – podkreślano znaczenie strategii, logistyki, finansów oraz organizacji państwowej. Kulminacją nowoczesnej refleksji nad wojną była teoria Carla von Clausewitza, który zdefiniował ją jako akt przemocy służący realizacji celów politycznych, podkreślając jej dynamiczny charakter oraz rolę niepewności. Równolegle rozwijały się inne koncepcje, takie jak ujęcie systemowe, manewrowe (Napoleon) czy materialno-organizacyjne.

W XIX i XX wieku pojawiają się dodatkowo interpretacje ideologiczne i społeczne, traktujące wojnę jako element walki klas lub długotrwały proces mobilizacji społecznej. Współczesne ujęcia rozszerzają jednak zakres konfliktu zbrojnego na działania nieregularne i podmioty niepaństwowe[1]. W rezultacie wojna jawi się jako zjawisko wielowymiarowe – polityczne, społeczne militarne, *quasi-militarne* – podczas gdy pokój pozostaje głównie kategorią normatywną.

W XXI wieku nic nie jest jasne, nie mamy nawet podstawowego modelu przedstawiającego przyszłą wojnę. Oblicze pola walki i działań wojennych ulega głębokiej transformacji napędzanej przez innowacje technologiczne. Współczesne bitwy są jest już definiowane wyłącznie przez działania militarne. Dlatego tradycyjne ujęcie kinetycznego rzeczywistości domeny kinetyczne zostaje wypierane na rzecz wojny hybrydowej czy cyberwojny. Zamiast tego w coraz większym

[1] W. Krzton, *Charakterystyczne cechy przeobrażeń współczesnych wojen i konfliktów zbrojnych* [w:] *Wojny i konflikty zbrojne XXI wieku,* red. J. Lasota, Warszawa 2015, s. 47-63.

stopniu kształtują je algorytmy cyfrowe, drony, narzędzia cybernetyczne oraz postęp naukowy, który sprawia, że przemoc stała się bardziej dostępna, precyzyjna i trudna do wyśledzenia. Zmiana ta nie ma charakteru wyłącznie taktycznego, lecz przekształca samą naturę konfliktu, umożliwiając nowym podmiotom i metodom podważanie tradycyjnych struktur konfliktów międzypaństwowych.

Jak trafnie zauważa Janusz Mucha, oprócz konfliktów militarnych istotną rolę w dzisiejszym świecie odgrywa konflikt społeczny. Zdaniem autora należy go rozumieć jak działania i walki różnych grup interesów, które rodzą stan wrogości lub współzawodnictwo[2]. Tak szerokie ujęcie pozwala na uwzględnienie zarówno źródeł konfliktu, jego przebiegu, jak i konsekwencji.

Celem monografii jest ukazanie ewolucji asymetryczności konfliktu, jak i jego wieloaspektowości. Przedmiotem badawczym są wybrane konflikty mające miejsce w XXI wieku o różnym podłożu. Już w tym miejscu warto postawić przykładowe pytania badawcze, na które autorzy-członkowie Koła Naukowego Polityki Bezpieczeństwa działającego na Politechnice Rzeszowskiej starali znaleźć się odpowiedzi:

1. Jakie są główne przyczyny konfliktów w XXI wieku?
2. Czy można wytyczyć granice informacyjne bezpieczeństwa państwa w dobie konfliktów?
3. Jak należy definiować wojnę hybrydową w konfliktach zbrojnych w dziejach ludzkości?
4. Dlaczego i w jakich uwarunkowaniach w określonych rejonach świata dochodzi do nasilenia konfliktów o charakterze zbrojnym, a kiedy o podłożu politycznym, społecznym, ekonomicznym czy cyberterrorystycznym?

Pomimo istnienia szerokiej literatury w tym zakresie autorzy rozdziałów podjęli kolejną próbę ukazania, jak istotnym elementem bezpieczeństwa świata jest asymetryczność zjawisk w tym konfliktów oraz czy można stawiać jasne granice terytorialne czy sieciocentryczne w tym zakresie. Zwrócili również uwagę w swoich wnioskach końcowych, że cyfryzacja stanowi w obliczu rosnących zmian technologicznych związanych z AI coraz większe zagrożenie i płaszczyznę konfliktów. Złożoność problemów występujących w infosferze jest niezwykle ważna, a przyczyną jej wzrostu jest brak świadomości samego zagrożenia na poziomie całej społeczności globalnej.

Publikacja ma charakter badawczy i jest skierowana do szerokiego grona czytelników, w tym studentów, doktorantów, jak i naukowców.

Izabela Oleksiewicz[3]

[2] J. Mucha, *Konflikt i społeczeństwo*, Warszawa 1976, s. 24.

[3] dr hab. Izabela Oleksiewicz, prof. PRz, Katedra Prawa i Administracji, Wydział Zarządzania, Politechnika Rzeszowska im. Ignacego Łukasiewicza. Opiekun Koła Naukowego Polityki Bezpieczeństwa Państwa. ORCID: 0000-0002-1622-7467.

Julia GAWRON[1]

KONFLIKTY POKOLEŃ JAKO PRZYKŁAD KONFLIKTÓW SPOŁECZNYCH W XXI WIEKU W POLSCE

W rozdziale przedstawiono zjawisko konfliktu międzypokoleniowego jako istotny element współczesnych przemian społecznych w Polsce. Ukazano jego źródła w różnicach doświadczeń historycznych, społecznych i kulturowych poszczególnych generacji, które wpływają na odmienne systemy wartości i sposoby postrzegania rzeczywistości. Omówiono główne obszary występowania napięć, takie jak rynek pracy, podejście do zdrowia psychicznego, zmiany językowe, funkcjonowanie mediów i polityki oraz model życia rodzinnego. Wskazano, że starsze pokolenia częściej preferują stabilność, lojalność i tradycyjne normy, natomiast młodsze wykazują większą elastyczność, mobilność oraz orientację na rozwój osobisty i równowagę między życiem zawodowym a prywatnym. Podkreślono również, że różnice te utrudniają komunikację, ale jednocześnie stanowią czynnik napędzający zmiany społeczne i kulturowe.

Słowa kluczowe: generacje, konflikt społeczny, wartości społeczne, tożsamość pokoleniowa.

Wprowadzenie

Konflikt pokoleń stanowi zjawisko trwale wpisane w funkcjonowanie społeczeństw. Od dawna obserwuje się napięcia między młodszymi a starszymi generacjami, wynikające z kwestionowania utrwalonych światopoglądów, ograniczeń oraz niechęci wobec zmian. Pomimo negatywnego wydźwięku samego pojęcia „konflikt", bywa on również interpretowany jako istotny element rozwoju społecznego i cywilizacyjnego, ponieważ krytyka wcześniejszych pokoleń często stanowi impuls do przemian w sferze wartości, norm i obyczajów. Konflikt międzypokoleniowy wynika w dużej mierze z naturalnych uwarunkowań życia społecznego. Jego podstawą jest dążenie młodszych pokoleń do emancypacji względem starszych, a także poszukiwanie własnego miejsca w strukturze społecznej oraz sposobu interpretacji otaczającej rzeczywistości[2].

Aby lepiej zrozumieć zjawisko konfliktu pokoleń, warto odwołać się do szerszej kategorii konfliktu społecznego. Konflikt społeczny to sytuacja lub proces zachodzący pomiędzy co najmniej dwoma podmiotami społecznymi, w którym pojawiają się sprzeczne interesy, wartości lub cele, przejawiające się zarówno

[1] Julia Gawron, studentka Politechniki Rzeszowskiej im. Ignacego Łukasiewicza, Koło Naukowe Polityki Bezpieczeństwa Państwa.

[2] https://poezja.org/wz/a/Motyw_konfliktu_pokolen/ (dostęp: 22.03.2026 r.).

w negatywnych postawach, jak i w działaniach o charakterze antagonistycznym[3]. W praktyce występuje wówczas, gdy realizacja celów jednej grupy społecznej odbywa się kosztem innych grup, uniemożliwiając im osiągnięcie własnych dążeń[4].

Definicja Lewisa A. Cosera ujmuje konflikt społeczny jako proces rywalizacji między podmiotami społecznymi, polegający na dążeniu do zdobycia wartości, pozycji społecznej, władzy oraz ograniczonych zasobów. Istotą tego procesu jest nie tylko osiągnięcie własnych celów, lecz także osłabienie, wyeliminowanie lub podporządkowanie strony przeciwnej[5].

Konflikt społeczny można zatem rozpatrywać w trzech podstawowych ujęciach. Po pierwsze, jako strukturalną sprzeczność wpisaną w system społeczny, wynikającą z ograniczonej dostępności pożądanych dóbr oraz wzajemnego wykluczania się celów poszczególnych grup. Po drugie, jako określony typ relacji i działań społecznych, przyjmujących formę walki lub współzawodnictwa. Po trzecie natomiast, jako stan wrogości i napięcia występujący pomiędzy jednostkami lub grupami społecznymi[6].

Wspomniane napięcia i sprzeczności interesów nabierają szczególnego charakteru w sytuacji, gdy ich źródłem staje się odmienność doświadczeń formacyjnych różnych grup wiekowych. W tym miejscu teoria konfliktu społecznego krzyżuje się z socjologią pokoleń, której podstawy teoretyczne zostały sformułowane przez Karla Mannheima. W jego ujęciu pokolenie stanowi zbiorowość osób urodzonych w zbliżonym okresie, między którymi kształtują się więzi oparte na wspólnocie doświadczeń życiowych. Istotną rolę odgrywa tu podobieństwo przeżyć historycznych oraz zbliżona sytuacja społeczna, które wpływają na formowanie się postaw, wartości i sposobów postrzegania rzeczywistości[7].

Pokolenie można również rozumieć jako grupę osób o podobnym umiejscowieniu w historycznym wymiarze procesu społecznego. Usytuowanie pokoleniowe należy pojmować jako dostęp do określonego zasobu potencjalnych doświadczeń, które kształtują charakterystyczne dla danej generacji sposoby myślenia, przeżywania oraz działania. Wynikają one z subiektywnie doświadczanego czasu oraz perspektywy uwarunkowanej miejscem jednostki w strukturze społeczno-historycznej[8].

Istotnym czynnikiem wpływającym na kształtowanie się konfliktów pokoleniowych w Polsce była transformacja ustrojowa zapoczątkowana w 1989 roku. Przemiany polityczne, gospodarcze i społeczne, związane z przejściem od systemu

---

[3] C. Fink, *Some Conceptual Difficulties in the Theory of Social Conflict,* "The Journal of Conflict Resolution, Journal of Peace Research" 1965, nr 4, s. 348-397.

[4] P.S. Cohen, *Modem Social Theory,* Londyn 1970, s. 184.

[5] L.A. Coser, *Conflict. Social Aspects* [w:] *International Encyclopedia of Social Sciences,* ed. David Sills, New York 1968, Vol. 3.

[6] J. Mucha, *Konflikt i społeczeństwo. Z problematyki konfliktu społecznego we współczesnych teoriach zachodnich*, PWN, Warszawa 1978, s. 8.

[7] K. Mannheim, *Problem pokoleń. Colloquia Communia* 1992-1993, nr 1-12, s. 144-147.

[8] K. Szafraniec, *Pokolenia i polskie zmiany: 45 lat badań wzdłuż czasu,* PWN, Warszawa 2022, s. 39.

centralnie planowanego do gospodarki rynkowej oraz demokratycznego porządku politycznego, doprowadziły do głębokiej redefinicji warunków życia społecznego. Zmiany te objęły m.in. rynek pracy, system wartości, struktury instytucjonalne oraz wzorce kariery zawodowej i stylu życia. W konsekwencji ukształtowały się odmienne doświadczenia życiowe poszczególnych generacji, co przyczyniło się do pogłębienia różnic w sposobach postrzegania rzeczywistości społecznej oraz oczekiwaniach wobec życia zawodowego i społecznego[9].

Pokolenia obecnie funkcjonujące w społeczeństwie można podzielić na kilka podstawowych kategorii, różniących się doświadczeniami historycznymi oraz systemem wartości. Przyjmuje się, że czas jednego pokolenia to około 25 lat[10]. Pokolenie Baby Boomers obejmuje osoby urodzone w latach 1946–1964 i kształtowane w realiach powojennych, często przywiązane do stabilności i tradycyjnych form organizacji życia społecznego[11]. Pokolenie X (1965–1980) dorastało w okresie dynamicznych przemian, cechując się pragmatyzmem oraz większą elastycznością wobec zmian[12]. Milenialsi, czyli pokolenie Y (1981–1994), rozwijali się w warunkach postępującej globalizacji i rozwoju technologii cyfrowych, co wpłynęło na ich otwartość oraz orientację na rozwój osobisty i równowagę między życiem zawodowym a prywatnym[13]. Z kolei pokolenie Z (1995–2010) funkcjonuje w pełni w środowisku cyfrowym, charakteryzując się wysokim poziomem kompetencji technologicznych, szybkim przetwarzaniem informacji oraz odmiennym podejściem do komunikacji i relacji społecznych[14].

Współistnienie tak zróżnicowanych grup w jednej przestrzeni sprawia, że współczesne konflikty społeczne w Polsce często przyjmują charakter pokoleniowy.

Praca zawodowa w rozumieniu pokoleń

Jednym z istotnych obszarów ujawniania się konfliktów międzypokoleniowych jest sfera pracy zawodowej, w szczególności podejście do lojalności wobec pracodawcy, gotowości do podejmowania nadgodzin oraz znaczenia równowagi między życiem zawodowym a prywatnym. Różnice w tych obszarach wynikają w dużej mierze z odmiennych doświadczeń historycznych oraz warunków społeczno-ekonomicznych, w których kształtowały się poszczególne pokolenia[15].

Starsze generacje, w szczególności osoby należące do pokolenia Baby Boomers oraz częściowo pokolenia X, dorastały i wchodziły na rynek pracy w okresie

[9] https://zpe.gov.pl/a/przeczytaj/DjmClE4ck (dostęp: 22.03.2026 r.).
[10] https://tropicieletalentow.pl/do-ktorego-pokolenia-nalezysz/ (dostęp: 22.03.2026 r.).
[11] https://www.ahe.lodz.pl/strefa-wiedzy/generacje (dostęp: 22.03.2026 r.).
[12] https://icomseo.pl/y-generation-pokolenie-y-czyli-millenialsi/ (dostęp: 22.03.2026 r.).
[13] Tamże.
[14] Tamże.
[15] J. Nowicka, *Pokolenia Baby Boomers, X, Y, Z na rynku pracy. Przypadek: branża TSL,* „Annales Universitatis Paedagogicae Cracoviensis, Studia de Cultura" 2025, 17(3), Akademia Nauk Stosowanych Angeliusa Silesiusa w Wałbrzychu, s. 59-60.

transformacji ustrojowej oraz niepewności gospodarczej lat 90. XX wieku. W tym kontekście praca była postrzegana przede wszystkim jako źródło stabilności ekonomicznej i bezpieczeństwa życiowego. Wysoka lojalność wobec pracodawcy, gotowość do poświęceń, w tym podejmowania nadgodzin oraz dążenie do długoterminowego zatrudnienia stanowiły istotne elementy budowania kariery zawodowej. Doświadczenia tego okresu ukształtowały przekonanie, że zaangażowanie i podporządkowanie się wymaganiom organizacji sprzyja utrzymaniu pozycji zawodowej[16].

W przeciwieństwie do tego młodsze pokolenia, w szczególności milenialsi oraz przedstawiciele pokolenia Z, funkcjonują w odmiennych realiach społeczno-gospodarczych, charakteryzujących się większą elastycznością rynku pracy, rozwojem technologii oraz innym podejściem do organizacji życia zawodowego. W ich przypadku praca coraz częściej traktowana jest jako narzędzie umożliwiające realizację celów życiowych, a nie jako wartość absolutna. W rezultacie większy nacisk kładzie się na zachowanie równowagi między życiem zawodowym a prywatnym (*work-life balance*), rozwój osobisty oraz ochronę zdrowia psychicznego. Przejawia się to m.in. w mniejszej skłonności do akceptowania nadgodzin oraz częstszej zmianie miejsca zatrudnienia[17].

Obecność na rynku pracy przedstawicieli różnych pokoleń wiąże się z dodatkowymi wyzwaniami organizacyjnymi i komunikacyjnymi. Każde z pokoleń reprezentuje odmienne systemy wartości, podejście do obowiązków zawodowych oraz inne oczekiwania wobec pracodawcy i współpracowników. Starsze pokolenia częściej preferują stabilność i przewidywalność, natomiast młodsze wykazują większą otwartość na zmiany i mobilność zawodową. Jednocześnie zróżnicowanie kompetencji i doświadczeń poszczególnych generacji może stanowić istotną wartość dla organizacji, choć wymaga odpowiedniego zarządzania i uwzględnienia różnic pokoleniowych w środowisku pracy[18].

Różnice w podejściu do pracy i lojalności wobec pracodawcy znajdują potwierdzenie również w danych empirycznych. W ciągu ostatnich trzech lat aż 38% Polaków zmieniło miejsce zatrudnienia, przy czym najwyższą mobilnością zawodową charakteryzują się osoby młode. Zmianę pracy deklaruje aż 85% osób w wieku 18–24 lata oraz 52% w grupie 25–34 lata. Szczególnie wysoki odsetek dotyczy osób na początkowym etapie kariery – wśród stażystów i pracowników na stanowiskach juniorskich aż 71% ma już za sobą zmianę pracodawcy. Dla porównania, wśród starszych specjalistów decyzję o zmianie zatrudnienia podjął jedynie co czwarty badany (25%)[19].

---

[16] Tamże.

[17] *Work-life balance w teorii i praktyce funkcjonowania współczesnych organizacji*, red. E. Szczygieł, T. Piecuch, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2019, s.49.

[18] J. Pawlak-Jęczewska, *Cztery pokolenia na rynku pracy*, „Informator Oświatowy. Biuletyn: Zróżnicowane potrzeby uczniów. Cyfryzacja edukacji" 2022, nr 1/22 (197), Ośrodek Doskonalenia Nauczycieli w Słupsku, s. 51.

[19] Badanie Pracuj.pl, https://media.pracuj.pl/427464-badanie-pracujpl-78-polakow-jest-otwartych-na-zmiane-pracy-a-co-trzeci-rozwaza-zatrudnienie-w-nowej-branzy (dostęp: 25.03.2026 r.).

Zjawisko to odzwierciedla wyraźne zróżnicowanie postaw wobec pracy w zależności od przynależności pokoleniowej. Dla młodszych generacji wysoka mobilność zawodowa stanowi naturalny etap kształtowania ścieżki kariery, związany z poszukiwaniem korzystniejszych warunków zatrudnienia, możliwości rozwoju oraz lepszego dopasowania pracy do indywidualnych oczekiwań. W podejściu tym widoczna jest również rosnąca popularność zjawiska określanego jako *quiet quitting*, polegającego na ograniczaniu zaangażowania zawodowego do zakresu formalnie wymaganych obowiązków. Natomiast starsze pokolenia częściej wykazują przywiązanie do stabilności zatrudnienia, traktując długotrwałą współpracę z jednym pracodawcą jako przejaw lojalności i odpowiedzialności zawodowej[20].

To, co dla przedstawicieli starszych pokoleń stanowi przejaw braku lojalności wobec pracodawcy oraz niestabilności zawodowej, dla młodszych generacji jest wyrazem troski o własny dobrostan oraz świadomego poszukiwania bardziej satysfakcjonujących warunków życia i pracy. Tak odmienne postrzeganie kariery zawodowej prowadzi do pogłębiających się trudności we wzajemnym zrozumieniu oraz utrudnia efektywną współpracę między przedstawicielami różnych pokoleń w ramach jednego zespołu[21].

Pokoleniowe różnice interpretacji jakości zdrowia

Kolejnym istotnym obszarem ujawniania się konfliktów międzypokoleniowych w Polsce jest podejście do zdrowia psychicznego oraz sposoby komunikowania emocji. Różnice w tym zakresie wynikają przede wszystkim z odmiennych norm kulturowych i społecznych, w których socjalizowały się poszczególne pokolenia[22].

W przypadku starszych generacji kwestie związane ze zdrowiem psychicznym przez długi czas pozostawały tematem tabu, rzadko podejmowanym zarówno w przestrzeni publicznej, jak i prywatnej. Problemy emocjonalne nie były zazwyczaj ujmowane w kategoriach medycznych, lecz interpretowane jako przejaw słabości, braku samodyscypliny czy niewystarczającej odporności psychicznej. W konsekwencji osoby doświadczające trudności rzadziej korzystały z profesjonalnej pomocy, a temat zdrowia psychicznego pozostawał marginalizowany[23].

Z kolei młodsze pokolenia, w szczególności przedstawiciele pokolenia Z w Polsce, funkcjonują w rzeczywistości, w której obserwuje się stopniową normalizację rozmów o zdrowiu psychicznym. Wzrasta świadomość społeczna dotycząca takich zjawisk jak depresja, zaburzenia lękowe czy wypalenie zawodowe,

---

[20] F. Lipiński, J. Koczy, *Zjawisko Quiet Quitting wśród polskich pracowników pokolenia Z,* „Academic Review of Business and Economics" 2023, Uniwersytet Ekonomiczny w Katowicach, s. 58-60.

[21] Tamże.

[22] E. Samardakiewicz-Kirol, K. Torres, *Wyjątkowi jak płatki śniegu,* https://zdalne.umlub.edu.pl/doc/dzjuml3/Wyjatkowi_jak_platki_sniegu.pdf (dostęp: 25.03.2026 r.).

[23] Tamże.

które coraz częściej postrzegane są jako problemy wymagające specjalistycznej diagnozy i wsparcia. Tendencję tę potwierdzają dane wskazujące na rosnącą liczbę osób korzystających z pomocy psychologicznej oraz zwiększoną liczbę przepisywanych leków przeciwdepresyjnych, szczególnie wśród osób młodych[24].

Dodatkowo napięcia te wzmacniane są przez język stosowany w debacie publicznej i codziennej komunikacji. Określenie „pokolenie płatków śniegu" (*snowflake generation*) funkcjonuje jako pejoratywne określenie młodszych generacji, sugerujące ich nadmierną wrażliwość i niską odporność psychiczną. Z kolei młodsze pokolenia posługują się terminem „boomer" w odniesieniu do starszych, często w celu zdyskredytowania ich poglądów jako przestarzałych i nieprzystających do współczesnych realiów. Tego rodzaju uproszczone i wartościujące etykiety dodatkowo utrudniają dialog międzypokoleniowy oraz pogłębiają istniejące podziały[25].

W konsekwencji to, co dla młodszych pokoleń stanowi przejaw świadomej troski o własny dobrostan i higienę psychiczną, w oczach starszych generacji bywa interpretowane jako brak odporności psychicznej czy tendencja do przyjmowania postawy nadmiernych oczekiwań. Zderzenie „kultury milczenia", charakterystycznej dla starszych pokoleń, z „kulturą autentyczności", reprezentowaną przez młodsze generacje, prowadzi do pogłębiania się nieporozumień w relacjach społecznych. W rezultacie, zamiast wzajemnego wsparcia, zarówno w środowisku rodzinnym, jak i zawodowym, pojawiają się wzajemne oskarżenia – z jednej strony o nadmierną wrażliwość, z drugiej zaś o brak empatii i zrozumienia[26].

Istotnym potwierdzeniem zmiany podejścia do zdrowia psychicznego wśród młodszych pokoleń są dane publikowane przez Narodowy Fundusz Zdrowia. W 2023 roku wsparciem objęto ponad 279 tysięcy dzieci i młodzieży, co stanowi wzrost o 134,6% w porównaniu z rokiem 2019, kiedy liczba ta wynosiła około 119 tysięcy. Równocześnie znacząco zwiększyły się nakłady finansowe na świadczenia psychiatryczne dla tej grupy – z niemal 260 mln zł w 2019 roku do ponad 1 mld zł w 2023 roku[27].

Podobną tendencję można zaobserwować w obszarze farmakoterapii. W 2023 roku refundowane leki przeciwdepresyjne wykupiło 1,7 mln osób, co oznacza wzrost o 83% w porównaniu z rokiem 2013. Szczególnie wyraźny jest ponad pięciokrotny wzrost liczby recept realizowanych dla dzieci i młodzieży poniżej 18. roku życia – z 15,9 tys. w 2013 roku do 84,6 tys. w 2023 roku[28].

---

[24] Tamże.

[25] *Diagnoza Młodzieży. Raport i rekomendacje,* red. P. Rabiej, Polskie Towarzystwo Polityki Społecznej, Warszawa 2026, s. 43-46.

[26] https://sukces.rp.pl/zdrowie-uroda/art43787701-mlode-pokolenie-nie-chce-sie-starzec-jak-rodzice-optymizacja-robi-furore (dostęp: 25.03.2026 r.).

[27] NFZ, Raporty i dane statystyczne dotyczące zdrowia psychicznego oraz refundacji leków przeciwdepresyjnych w Polsce, https://www.nfz.gov.pl/aktualnosci/aktualnosci-centrali/kryzys-psychiczny-u-dzieci-i-mlodziezy-jak-go-rozpoznac-i-gdzie-szukac-pomocy,8683.html (dostęp: 25.03.2026 r.).

[28] Tamże.

Zjawiska te można interpretować jako przejaw rosnącej świadomości znaczenia zdrowia psychicznego oraz większej gotowości młodszych pokoleń do korzystania z profesjonalnej pomocy. Jednocześnie stanowią one istotne źródło napięć międzypokoleniowych. Dla młodszych generacji korzystanie z terapii czy leczenia psychiatrycznego jest działaniem racjonalnym i odpowiedzialnym, wpisującym się w dbałość o własny dobrostan, natomiast dla części przedstawicieli starszych pokoleń wzrost liczby diagnoz oraz form wsparcia może być postrzegany jako przejaw nadmiernej wrażliwości lub osłabienia odporności psychicznej.

W rezultacie dane te nie tylko obrazują skalę zmian społecznych, ale również ukazują pogłębiające się różnice w sposobie rozumienia zdrowia psychicznego, co prowadzi do trudności komunikacyjnych oraz wzmacnia istniejące konflikty międzypokoleniowe.

Język ojczysty jako konflikt pokoleń

Kolejną płaszczyzną konfliktu międzypokoleniowego w Polsce jest podejście do ewolucji normy językowej. Język przestał być jedynie narzędziem komunikacji, a stał się polem walki o wartości. W ostatnich latach obserwuje się intensywną debatę dotyczącą ewolucji języka, obejmującą takie zagadnienia jak stosowanie feminatywów, użycie form neutralnych płciowo czy dobór zaimków. Spory te wykraczają poza kwestie czysto lingwistyczne i stają się elementem szerszych przemian społecznych oraz kulturowych[29].

W ujęciu ogólnym można wyróżnić dwie przeciwstawne postawy wobec tych zmian. Pierwsza z nich, określana jako konserwatyzm językowy, zakłada przywiązanie do tradycyjnych norm językowych i traktuje nowe formy jako nieuzasadnione ingerencje w system języka, a niekiedy wręcz jako jego „zniekształcanie" lub „niszczenie". Druga postawa, o charakterze progresywnym, postrzega język jako narzędzie kształtowania rzeczywistości społecznej, które powinno uwzględniać różnorodność społeczną i przeciwdziałać wykluczeniu, w tym dyskryminacji ze względu na płeć czy tożsamość[30].

Napięcia te znajdują odzwierciedlenie zarówno w debacie publicznej, jak i w działaniach instytucjonalnych. Przykładem są dyskusje prowadzone w ramach Rady Języka Polskiego, które dotyczą m.in. zasadności wprowadzania i upowszechniania form żeńskich w języku polskim. Równolegle podobne spory toczą się w przestrzeni medialnej i w mediach społecznościowych, gdzie kwestie poprawności językowej oraz tzw. poprawności politycznej często stają się przedmiotem intensywnych debat[31].

---

[29] https://www.wirtualnemedia.pl/jezykowe-konflikty-miedzypokoleniowe,7177871409059969a (dostęp: 25.03.2026 r.).

[30] S. Dubisz, *Najnowsze dzieje języka polskiego (1918-2018)*, „Poradnik Językowy" 2022, nr 10, s. 15-23.

[31] Rada Języka Polskiego przy Prezydium PAN. Stanowisko Rady Języka Polskiego w sprawie żeńskich form nazw zawodów i tytułów, przyjęte na posiedzeniu plenarnym Rady 19 marca 2012

Na współczesne postrzeganie języka jako obszaru napięć społecznych wskazują również wyniki badań opinii publicznej. W badaniu przeprowadzonym w dniach 19–22 stycznia 2024 roku na ogólnopolskiej próbie 1054 osób dorosłych wykazano, że kwestie językowe mogą stanowić realne źródło konfliktów. Co trzeci respondent przyznał, że rozmowy o języku polskim prowadzą do sporów z członkami rodziny lub znajomymi, co potwierdza ich znaczenie także w relacjach międzypokoleniowych[32].

Uzyskane wyniki ukazują wyraźne zróżnicowanie postaw wobec zmian językowych. Z jednej strony dostrzegalna jest rosnąca obecność feminatywów, co odzwierciedla zachodzące przemiany społeczne. Z drugiej strony zauważalny jest opór wobec bardziej radykalnych form, takich jak konstrukcje neutralne płciowo (tzw. osobatywy), co świadczy o przywiązaniu części społeczeństwa do tradycyjnej normy językowej[33].

Interesujące są także zmiany w sposobach korzystania ze źródeł wiedzy o języku. Zarówno młodsze, jak i starsze pokolenia częściej wykorzystują narzędzia cyfrowe niż tradycyjne słowniki, co wskazuje na transformację praktyk komunikacyjnych. Jednocześnie język polski jest częściej kojarzony z tradycją niż z nowoczesnością, co może sprzyjać zachowawczemu podejściu do jego przekształceń[34].

Ciekawym i nowym wymiarem tego sporu jest tzw. wojna o nazewnictwo produktów roślinnych. Debata publiczna wokół prób zakazu używania określeń takich jak „*wege-burger*" czy „szynka sojowa" stanowi klasyczny przykład konfliktu pokoleniowo-legislacyjnego. Starsze pokolenia, często przywiązane do tradycyjnych kategorii kulinarnych, postrzegają te nazwy jako wprowadzanie konsumenta w błąd. Z kolei młodzi Polacy, wśród których dieta roślinna jest znacznie popularniejsza, widzą w takich zakazach niepotrzebną próbę hamowania zmian światopoglądowych i ekologicznych za pomocą narzędzi językowych[35].

Polityka i media

Istotnym obszarem ujawniania się konfliktów międzypokoleniowych w Polsce jest sfera polityki oraz mediów, które mają duży wpływ na kształtowanie postaw społecznych i światopoglądowych. Różnice pokoleniowe w tym zakresie

roku, „Język Polski" – organ Towarzystwa miłośników języka polskiego – wydanie publikacji dofinansowało Ministerstwo Nauki i Szkolnictwa Wyższego, Uniwersytet Jagielloński, Kraków 2021, s.230-231.

[32] *Postawy Polaków wobec zmian w języku. Raport z badania ilościowego dla Rady Języka Polskiego*, red. E. Kołodziejek, R. Zimny, Prezydium PAN, Warszawa 2024, s. 5-20.

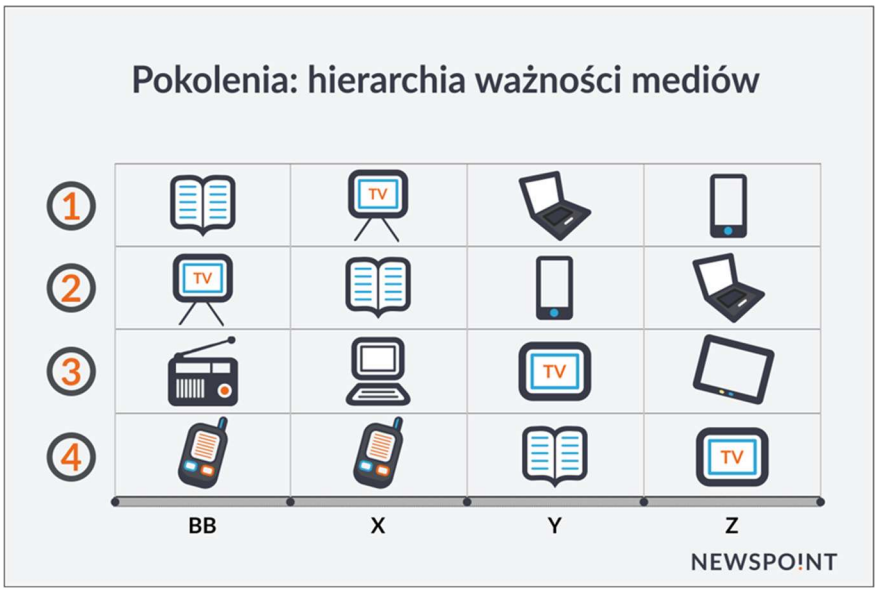
[33] Tamże.

[34] Tamże.

[35] https://www.green-news.pl/4384-spor-o-nazwy-dla-miesa-roslinnego-w-unii-europejskiej (dostęp: 28.03.2026 r.).

dotyczą zarówno sposobów pozyskiwania informacji, jak i preferencji politycznych oraz poziomu zaangażowania obywatelskiego[36].

Starsze pokolenia częściej korzystają z tradycyjnych źródeł informacji, takich jak telewizja, radio czy prasa, które charakteryzują się bardziej jednokierunkowym przekazem. W ich przypadku media pełnią funkcję głównego źródła wiedzy o świecie społecznym i politycznym. Z kolei młodsze generacje, w szczególności przedstawiciele pokolenia Y i Z, funkcjonują w środowisku cyfrowym, w którym dominującą rolę odgrywają media społecznościowe oraz internetowe serwisy informacyjne. Przekaz medialny ma tu charakter bardziej zróżnicowany, interaktywny i często spersonalizowany[37].



Rys. 1. Hierarchia wartości mediów według członków pokoleń

Źródło: https://www.newspoint.pl/blog/raport-newspoint-pokolenia-w-polsce-i-potrzeba-monitorowania-ich-rosnacej-aktywnosci

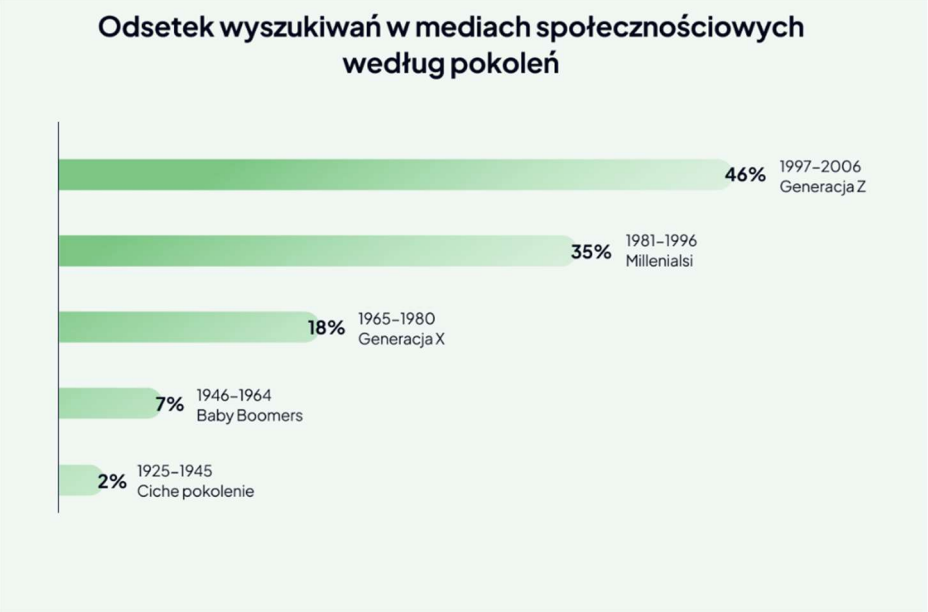
Potwierdza to również hierarchia ważności mediów, która wskazuje, że starsze pokolenia preferują tradycyjne źródła informacji, podczas gdy młodsze koncentrują się na mediach cyfrowych i mobilnych. Różnice te przekładają się na odmienne postrzeganie rzeczywistości społeczno-politycznej – młodsze pokolenia częściej uczestniczą w dyskusjach online, angażują się w działania o charakterze

[36] S. Lyons, L. Kuron, *Generational differences in the workplace: A review of the evidence and directions for future Research,* "Journal of Organizational Behavior" 2014, nr 1, s. 139-157.

[37] D. Puchalska, *Media społecznościowe a zjawisko ekshibicjonizmu społecznego w pokoleniach Z oraz Baby Boomers,* Wyższa Szkoła Informatyki i Zarządzania z siedzibą w Rzeszowie, Rzeszów 2024, s. 51-55.

społecznym oraz wykazują większą otwartość na kwestie związane z prawami mniejszości, zmianami klimatycznymi czy równością społeczną, podczas gdy starsze generacje częściej odwołują się do tradycyjnych wartości oraz stabilności systemu społecznego i politycznego[38].

Pokolenie Z, choć wciąż korzysta z Google, znacznie częściej wybiera media społecznościowe jako główne źródło wyszukiwania informacji w Internecie.



Rys. 2. Odsetek wyszukiwań w mediach społecznościowych według członków pokoleń

Źródło: https://www.sempire.pl/czy-pokolenie-z-wciaz-korzysta-z-google-nowe-sposoby-wyszukiwania.html

Różnice międzypokoleniowe w sposobie korzystania z mediów znajdują również potwierdzenie w danych dotyczących aktywności w mediach społecznościowych. Analiza odsetka wyszukiwań w tych mediach wskazuje na wyraźną dominację młodszych pokoleń. W przypadku pokolenia Z udział ten wynosi aż 46%, podczas gdy wśród milenialsów 35%. Dla porównania, w pokoleniu X jest to 18%, natomiast wśród Baby Boomers jedynie 7%, a w najstarszej grupie zaledwie 2%[39].

Dane te wyraźnie ukazują, że młodsze pokolenia znacznie częściej traktują media społecznościowe jako podstawowe źródło informacji i przestrzeń aktywności społecznej. W konsekwencji ich obraz rzeczywistości społeczno-politycznej

[38] Tamże.

[39] *Czy pokolenie Z wciąż korzysta z Google? Nowe sposoby wyszukiwania*, https://www.sempire.pl/czy-pokolenie-z-wciaz-korzysta-z-google-nowe-sposoby-wyszukiwania.html (dostęp: 25.03.2026 r.).

kształtowany jest w dużej mierze przez treści internetowe, które mają charakter szybki, zróżnicowany i często spersonalizowany. Z kolei starsze pokolenia, w znacznie mniejszym stopniu obecne w mediach społecznościowych, częściej opierają się na przekazie tradycyjnych mediów[40].

Tak wyraźne różnice w sposobach pozyskiwania informacji sprzyjają powstawaniu odmiennych „światów informacyjnych", co utrudnia dialog międzypokoleniowy oraz pogłębia istniejące podziały polityczne. W rezultacie media – zamiast pełnić funkcję integrującą – stają się czynnikiem wzmacniającym konflikty międzypokoleniowe, szczególnie w kontekście interpretacji wydarzeń politycznych i społecznych[41].

Konflikt międzypokoleniowy w tym obszarze przejawia się również w sposobie interpretacji wydarzeń politycznych oraz oceny instytucji publicznych. Różnice te prowadzą do polaryzacji opinii, utrudniają dialog oraz sprzyjają powstawaniu tzw. baniek informacyjnych, w których poszczególne grupy funkcjonują w odmiennych rzeczywistościach informacyjnych[42].

Różnice międzypokoleniowe w sferze polityki znajdują również potwierdzenie w danych empirycznych. Badania prowadzone przez Centrum Badania Opinii Społecznej wskazują na wyraźne zmiany w autoidentyfikacji politycznej młodych Polaków w ostatnich latach. W okresie 2019-2020 odsetek osób w wieku 18–24 lata deklarujących poglądy lewicowe wzrósł z 17% do 30%, podczas gdy identyfikacja z prawicą zwiększyła się z 23% do 27%. Oznacza to, że w tej grupie wiekowej po raz pierwszy od wielu lat zaobserwowano przewagę deklaracji lewicowych nad prawicowymi. Zjawisko to nabiera szczególnego znaczenia w zestawieniu z poglądami ogółu społeczeństwa, w którym nadal dominują orientacje prawicowe (37%), wyraźnie przewyższające odsetek identyfikacji lewicowych (20%). Wskazuje to na rosnącą rozbieżność światopoglądową między młodszymi a starszymi pokoleniami[43].

Zakładanie rodziny

Współczesne przemiany społeczne prowadzą do wyraźnego zróżnicowania postaw wobec rodziny pomiędzy poszczególnymi pokoleniami. Konflikt ten dotyczy przede wszystkim rozumienia roli rodziny, momentu jej zakładania oraz znaczenia instytucji małżeństwa. Starsze pokolenia częściej reprezentują tradycyjny model rodziny, oparty na wczesnym zawieraniu małżeństw, trwałości związku

[40] Tamże.

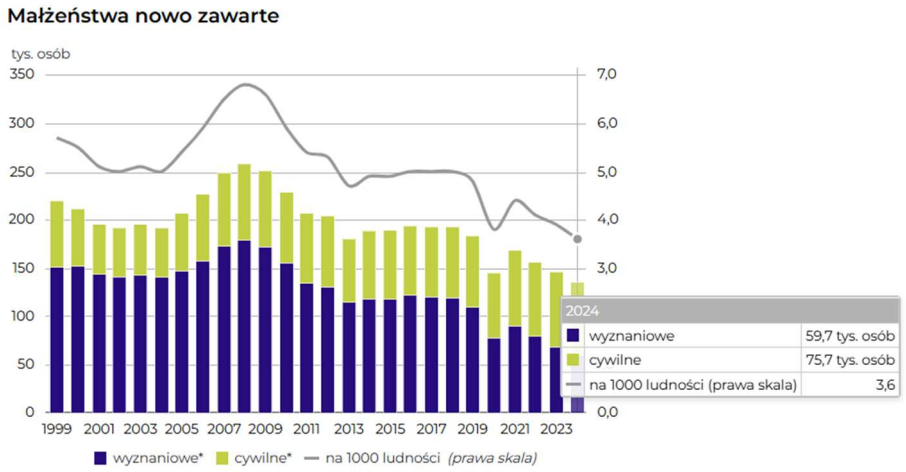
[41] J. Idzik, R. Klepka, *Bańka informacyjna i zjawisko echo chamber* [w:] *Encyklopedia bezpieczeństwa*, red. O. Wasiuta, S. Wasiuta, t. 1, Wyd. Libron, Kraków 2021, s. 204-205.

[42] Tamże.

[43] Centrum Badania Opinii Społecznej. Ważne kwestie społeczno-polityczne w opiniach młodych Polaków. Komunikat z badań nr 93/2021, Fundacja Centrum Badania Opinii Społecznej, Warszawa 2021, s. 1.

oraz większej liczbie dzieci. Rodzina stanowi w tym ujęciu podstawową wartość społeczną i stabilizującą jednostkę strukturę życia społecznego[44].

Z kolei młodsze pokolenia prezentują bardziej elastyczne podejście do kwestii życia rodzinnego. Obserwuje się wyraźną tendencję do opóźniania decyzji o zawarciu małżeństwa oraz posiadaniu dzieci, co wiąże się z wydłużeniem okresu edukacji, rozwojem kariery zawodowej oraz dążeniem do samorealizacji. Coraz częściej akceptowane są również alternatywne formy życia rodzinnego, takie jak związki nieformalne czy życie w pojedynkę. Zjawiska te wpisują się w szersze procesy indywidualizacji oraz przemian kulturowych charakterystycznych dla społeczeństw nowoczesnych[45].



Rys. 3. Liczba nowo zawartych małżeństw na przestrzeni lat

Źródło: Główny Urząd Statyczny.

Z danych Głównego Urzędu Statystycznego wynika, że w 2025 roku zawarto około 133 tys. związków małżeńskich, co oznacza niewielki spadek w porównaniu z rokiem poprzednim. Współczynnik małżeństw utrzymał się na poziomie około 3,6‰, a częstość ich zawierania była zbliżona zarówno w miastach, jak i na obszarach wiejskich[46].

Struktura zawieranych małżeństw wskazuje na istotne zróżnicowanie społeczne i kulturowe. W 2024 roku około 44% stanowiły małżeństwa wyznaniowe, przy czym na wsi ich udział był wyraźnie wyższy i wynosił około 56%.

[44] https://publikacje.edu.pl/jak-wyglada-tradycyjny-model-rodziny-struktura-i-przemiany#:~:text=Tradycyjna%20rodzina%20wywodzi%20si%C4%99%20z%20czas%C3%B3w%2C%20kiedy,opiera%C5%82a%20si%C4%99%20na%20ziemi%20i%20pracy%20w%C5%82asnej (dostęp: 28.03.2025 r.).

[45] Tamże.

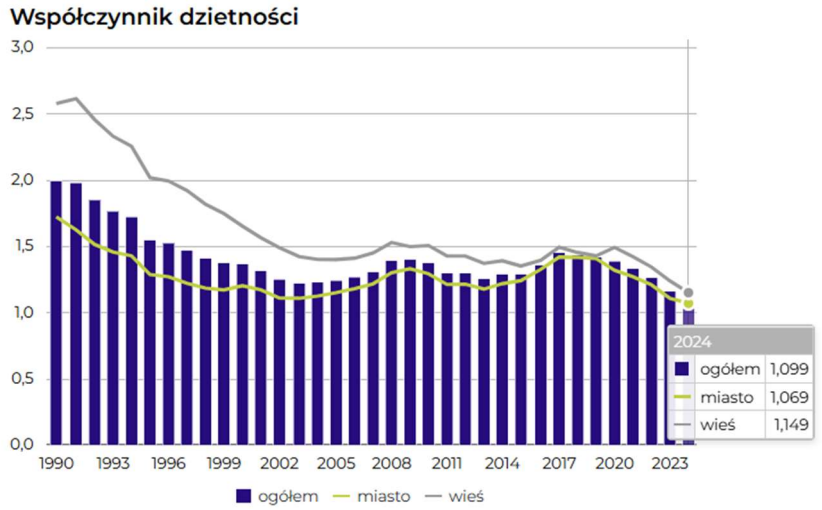
[46] GUS, https://ssgk.stat.gov.pl/Ludnosc.html (dostęp: 18.03.2026 r.).

Jednocześnie większość nowo zawieranych związków (około 73%) to małżeństwa pierwsze, co oznacza, że są one zawierane przez osoby wcześniej niepozostające w formalnych relacjach małżeńskich[47].

Na szczególną uwagę zasługuje wzrost wieku nowożeńców. W 2024 roku mediana wieku mężczyzn zawierających małżeństwo wyniosła 32 lata, natomiast kobiet – prawie 30 lat, co oznacza wzrost o około 6 lat w porównaniu z początkiem XXI wieku. Tendencja ta potwierdza obserwowane wśród młodszych pokoleń przesuwanie decyzji o formalizacji związku na późniejsze etapy życia. Dodatkowo nowożeńcy zamieszkujący miasta byli przeciętnie starsi o około 2 lata niż osoby z obszarów wiejskich[48].

Przedstawione dane wskazują, że zmiany w zakresie zawierania małżeństw, podobnie jak w przypadku dzietności, odzwierciedlają przemiany stylów życia oraz systemów wartości młodszych pokoleń. Opóźnianie decyzji o małżeństwie oraz spadek liczby zawieranych związków formalnych stanowią istotny przejaw współczesnego konfliktu pokoleń w podejściu do rodziny.

Istotnym wymiarem konfliktu pokoleń w tym obszarze jest także zróżnicowanie systemów wartości. Starsze generacje częściej postrzegają rodzinę jako obowiązek społeczny i naturalny etap życia, podczas gdy młodsze traktują ją jako jedną z wielu możliwych dróg realizacji życiowej. Różnice te prowadzą niekiedy do napięć międzypokoleniowych, zwłaszcza w kontekście oczekiwań dotyczących zawarcia małżeństwa czy posiadania potomstwa[49].



Rys. 4. Dane dotyczące współczynnika dzietności

Źródło: Główny Urząd Statyczny.

[47] Tamże.
[48] Tamże.
[49] https://styl.interia.pl/spoleczenstwo/news-koniec-wolnosci-i-mnostwo-wydatkow-czy-rzeczy-wiscie-pokoleni,nId,21396384 (dostęp: 18.03.2026 r.).

Analiza danych demograficznych dotyczących Polski wskazuje na wyraźne zmiany w zrachowaniach prokreacyjnych społeczeństwa. Według wstępnych szacunków publikowanych przez Główny Urząd Statystyczny w 2025 roku zarejestrowano około 238 tys. urodzeń żywych, co oznacza spadek o około 14 tys. w porównaniu z rokiem poprzednim. Jednocześnie współczynnik urodzeń obniżył się do poziomu 6,4‰[50].

Szczególnie istotnym wskaźnikiem jest współczynnik dzietności, który spadł z 1,16 w 2023 roku do 1,10 w 2024 roku. Oznacza to, że na 100 kobiet w wieku rozrodczym przypada około 110 urodzonych dzieci, przy czym widoczne jest zróżnicowanie pomiędzy miastem (107) a wsią (115). Wartość ta pozostaje znacząco poniżej poziomu zastępowalności pokoleń, co wskazuje na utrwalający się trend ograniczania liczby urodzeń[51].

Przytoczone dane statystyczne potwierdzają, że zmiany w podejściu do rodziny wśród młodszych pokoleń mają charakter nie tylko deklaratywny, lecz znajdują odzwierciedlenie w rzeczywistych zrachowaniach demograficznych. Spadek liczby urodzeń oraz obniżenie współczynnika dzietności wskazują na przesuwanie decyzji o rodzicielstwie lub rezygnację z niego, co pozostaje w ścisłym związku z przemianami wartości, stylów życia oraz ról społecznych. W konsekwencji konflikt pokoleń w tym obszarze nabiera wymiaru strukturalnego i stanowi jeden z elementów współczesnych przemian społecznych w Polsce.

Ważnym czynnikiem wpływającym na zmianę podejścia do rodziny jest również transformacja ról społecznych, w szczególności roli kobiet. W tradycyjnym modelu rodziny kobieta była przede wszystkim odpowiedzialna za prowadzenie gospodarstwa domowego oraz wychowanie dzieci. Współcześnie coraz większe znaczenie ma aktywność zawodowa kobiet, ich niezależność ekonomiczna oraz dążenie do samorealizacji poza sferą życia rodzinnego. Prowadzi to do przekształcenia modelu rodziny w kierunku bardziej partnerskiego układu relacji, co nie zawsze jest zgodne z oczekiwaniami starszych pokoleń[52].

Zmiany te wpływają nie tylko na strukturę rodziny, ale również na sposób jej postrzegania w społeczeństwie. Rodzina przestaje być jedynym dominującym wzorcem organizacji życia prywatnego, a staje się jedną z wielu możliwych form realizacji potrzeb jednostki. W konsekwencji pogłębia się dystans pomiędzy pokoleniami, którego źródłem są odmienne doświadczenia społeczne oraz różne konteksty kulturowe kształtujące ich postawy[53].

---

[50] GUS, https://ssgk.stat.gov.pl/Ludnosc.html (dostęp: 18.03.2026 r.).

[51] Tamże.

[52] Ł.P. Ratajczak, A. Kozłowska, *Zmiana modelu ojcostwa. W stronę równoważenia ról rodzicielskich i budowania równowagi pomiędzy życiem zawodowym a rodzinnym*, „Resocjalizacja Polska" 2023, nr 26, s. 239.

[53] Tamże.

Podsumowanie

Konflikt międzypokoleniowy jest stałym i nieuniknionym zjawiskiem w życiu społecznym, które w realiach XXI wieku można postrzegać jako jedną z ważniejszych odmian konfliktów społecznych. Wynika on z odmiennych doświadczeń historycznych, warunków społeczno-ekonomicznych oraz procesów kulturowych kształtujących poszczególne generacje. Różnice te znajdują odzwierciedlenie w ważnych obszarach życia społecznego, takich jak rynek pracy, podejście do zdrowia psychicznego, język, sfera polityczno-medialna oraz model życia rodzinnego, gdzie ujawniają się odmienne systemy wartości, normy oraz sposoby interpretowania rzeczywistości[54].

Współczesny charakter konfliktu międzypokoleniowego w Polsce pozostaje ściśle związany z dynamicznymi przemianami społecznymi, w szczególności z transformacją ustrojową oraz rozwojem technologii cyfrowych, które doprowadziły do pogłębienia różnic w stylach życia, oczekiwaniach oraz sposobach funkcjonowania jednostek. W konsekwencji przedstawiciele różnych pokoleń coraz częściej operują odmiennymi kategoriami interpretacyjnymi, co utrudnia wzajemne porozumienie i sprzyja powstawaniu napięć charakterystycznych dla współczesnych konfliktów społecznych[55].

Jednocześnie konflikt międzypokoleniowy nie powinien być ujmowany wyłącznie w kategoriach zjawiska destabilizującego. Stanowi on również istotny mechanizm zmian społecznych, umożliwiający redefinicję obowiązujących norm i wartości oraz ich dostosowanie do zmieniających się realiów. Napięcia między pokoleniami odzwierciedlają proces negocjowania znaczeń, typowy dla społeczeństw XXI wieku, w którym ścierają się dążenia do zachowania ciągłości z potrzebą adaptacji i innowacji[56].

Zasadniczym wyzwaniem pozostaje ograniczona zdolność do prowadzenia konstruktywnego dialogu międzygeneracyjnego. Utrwalone schematy interpretacyjne, uproszczone etykiety oraz brak otwartości na odmienne doświadczenia sprzyjają pogłębianiu dystansu społecznego, przez co różnice, które mogłyby stanowić źródło komplementarności, stają się czynnikiem podziałów[57].

Należy przy tym podkreślić, że wyróżnione kategorie pokoleniowe mają charakter analitycznego uogólnienia. Przynależność do określonej generacji nie przesądza w sposób jednoznaczny o postawach i zrachowaniach jednostki, która pozostaje kształtowana przez zróżnicowane doświadczenia indywidualne i społeczne.

---

[54] M. Ryś, *Konflikty w rodzinie, niszczą czy budują?* Centrum Metodyczne Pomocy Psychologiczno-Pedagogicznej Ministerstwa Edukacji Narodowej, Warszawa 1998, s. 19.

[55] E. Wiśniewska, *Starsi i młodsi w dialogu międzypokoleniowym,* „Społeczeństwo. Edukacja. Język" 2017, t. 6, Państwowa Wyższa Szkoła Zawodowa w Płocku, s. 27-28.

[56] E. Roszkowska, *Rozwój społeczny a rozwiązywanie konfliktów społecznych* [w:] *Rozwój regionalny a rozwój społeczny*, red. A.F. Bocian, Białystok 2006, s. 267-270.

[57] E. Wiśniewska, *Starsi i młodsi w dialogu…,* dz. cyt., s. 37.

Ujęcie to pozwala jednak uchwycić dominujące tendencje i wzorce, szczególnie widoczne w obrębie centralnych roczników danego pokolenia[58].

W tym kontekście szczególnego znaczenia nabiera potrzeba rozwijania kompetencji komunikacyjnych oraz budowania przestrzeni sprzyjającej wymianie perspektyw. Uznanie zróżnicowania doświadczeń jako wartości, a nie bariery, może przyczynić się do ograniczenia napięć oraz lepszego wykorzystania potencjału wynikającego z różnorodności pokoleniowej. Konflikt pokoleń jawi się zatem jako zjawisko ambiwalentne, czyli jednocześnie generujące napięcia i stanowiące jeden z głównych mechanizmów dynamiki współczesnych społeczeństw[59]

Bibliografia

Cohen P.S., *Modem Social Theory*, Londyn 1970.

Coser L.A., *Conflict. Social Aspects* [w:] *International Encyclopedia of Social Sciences*, ed. D. Sills, New York 1968, Vol. 3.

Dubisz S., *Najnowsze dzieje języka polskiego (1918-2018),* „Poradnik Językowy" 2022, nr 10.

Filip O., Kaźmierczak N., *Różnice w komunikacji między pokoleniami. Jak Pokolenie X, Millenialsi i Generacja Z postrzegają i stosują różne style komunikacyjne?* „Edukacja Dziecka" 2025, nr 9.

Fink C., *Some Conceptual Difficulties in the Theory of Social Conflict,* "The Journal of Conflict Resolution, Journal of Peace Research" 1965, nr 4.

Idzik J., Klepka R., *Bańka informacyjna i zjawisko echo chamber* [w:] *Encyklopedia bezpieczeństwa*, red. O. Wasiuta, S. Wasiuta, t. 1, Wyd. Libron, Kraków 2021.

Postawy Polaków wobec zmian w języku. Raport z badania ilościowego dla Rady Języka Polskiego, red. E. Kołodziejek, R. Zimny, Prezydium PAN, Warszawa 2024.

Lipiński F., Julianna Koczy J., *Zjawisko Quiet Quitting wśród polskich pracowników pokolenia Z,* „Academic Review of Business and Economics" 2023, Uniwersytet Ekonomiczny w Katowicach.

Lyons S., Kuron L., *Generational differences in the workplace: A review of the evidence and directions for future Research*, "Journal of Organizational Behavior" 2014, nr 1.

Mannheim K., *Problem pokoleń,* „Colloquia Communia" 1992–1993, nr 1–12.

Mucha J., *Konflikt i społeczeństwo. Z problematyki konfliktu społecznego we współczesnych teoriach zachodnich*, PWN, Warszawa 1978.

Nowicka J*., Pokolenia Baby Boomers, X, Y, Z na rynku pracy. Przypadek: branża TSL,* „Annales Universitatis Paedagogicae Cracoviensis, Studia de Cultura" 2025, 17(3), Akademia Nauk Stosowanych Angeliusa Silesiusa w Wałbrzychu

Pawlak-Jęczewska J., *Cztery pokolenia na rynku pracy*, „Informator Oświatowy" – Biuletyn: Zróżnicowane potrzeby uczniów. Cyfryzacja edukacji 2022, nr 1/22 (197), Ośrodek Doskonalenia Nauczycieli w Słupsku.

[58] https://www.newspoint.pl/blog/raport-newspoint-pokolenia-w-polsce-i-potrzeba-monitorowania-ich-rosnacej-aktywnosci (dostęp: 18.03.2026 r.).

[59] https://zwierciadlo.pl/psychologia/536676,1,kiedy-ja-bylam-w-twoim-wieku-konflikt-pokolen-czyli-jak-nie-zostac-dziadersem.read (dostęp: 30.03.2026 r.).

Puchalska D., *Media społecznościowe a zjawisko ekshibicjonizmu społecznego w pokoleniach Z oraz Baby Boomers,* Wyższa Szkoła Informatyki i Zarządzania z siedzibą w Rzeszowie, Rzeszów 2024.

Diagnoza Młodzieży. Raport i rekomendacje, red. P. Rabiej, Polskie Towarzystwo Polityki Społecznej, Warszawa 2026.

Rada Języka Polskiego przy Prezydium PAN, *Stanowisko Rady Języka Polskiego w sprawie żeńskich form nazw zawodów i tytułów, przyjęte na posiedzeniu plenarnym Rady 19 marca 2012 roku,* „Język Polski" – organ Towarzystwa miłośników języka polskiego wydanie publikacji dofinansowało Ministerstwo Nauki i Szkolnictwa Wyższego, Uniwersytet Jagielloński, Kraków 2022.

Ratajczak Ł.P., Kozłowska A., *Zmiana modelu ojcostwa. W stronę równoważenia ról rodzicielskich i budowania równowagi pomiędzy życiem zawodowym a rodzinnym,* „Resocjalizacja Polska" 2023, nr 26.

Roszkowska E., *Rozwój społeczny a rozwiązywanie konfliktów społecznych* [w:] *Rozwój regionalny a rozwój społeczny*, red. A.F. Bocian, Białystok 2006.

Ryś M., *Konflikty w rodzinie, niszczą czy budują?* Centrum Metodyczne Pomocy Psychologiczno-Pedagogicznej Ministerstwa Edukacji Narodowej, Warszawa 1998.

Szafraniec K., *Pokolenia i polskie zmiany: 45 lat badań wzdłuż czasu,* PWN, Warszawa 2022.

Work-life balance w teorii i praktyce funkcjonowania współczesnych organizacji, red. E. Szczygieł, T. Piecuch, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2019.

Wiśniewska E., *Starsi i młodsi w dialogu międzypokoleniowym,* „Społeczeństwo. Edukacja. Język" 2017, t. 6, Państwowa Wyższa Szkoła Zawodowa w Płocku.

Dane statystyczne

Centrum Badania Opinii Społecznej, *Ważne kwestie społeczno-polityczne w opiniach młodych Polaków. Komunikat z badań nr 93/2021*, Fundacja Centrum Badania Opinii Społecznej, Warszawa 2021.

GUS, https://ssgk.stat.gov.pl/Ludnosc.html

Narodowy Fundusz Zdrowia, Raporty i dane statystyczne dotyczące zdrowia psychicznego oraz refundacji leków przeciwdepresyjnych w Polsce, https://www.nfz.gov.pl/aktualnosci/aktualnosci-centrali/kryzys-psychiczny-u-dzieci-i-mlodziezy-jak-go-rozpoznac-i-gdzie-szukac-pomocy,8683.html

Netografia

Badanie https://media.pracuj.pl/427464-badanie-pracujpl-78-polakow-jest-otwartych-na-zmiane-pracy-a-co-trzeci-rozwaza-zatrudnienie-w-nowej-branzy

Czy pokolenie Z wciąż korzysta z Google? Nowe sposoby wyszukiwania, https://www.sempire.pl/czy-pokolenie-z-wciaz-korzysta-z-google-nowe-sposoby-wyszukiwania.html

https://poezja.org/wz/a/Motyw_konfliktu_pokolen/

https://publikacje.edu.pl/jak-wyglada-tradycyjny-model-rodziny-struktura-iprzemiany#:~:text=Tradycyjna%20rodzina%20wywodzi%20si%C4%99%20z%20czas%C3%B3w%2C%20kiedy,opiera%C5%82a%20si%C4%99%20na%20ziemi%20i%20pracy%20w%C5%82asnej

https://styl.interia.pl/spoleczenstwo/news-koniec-wolnosci-i-mnostwo-wydatkow-czy-rzeczywiscie-pokoleni,nId,21396384

https://sukces.rp.pl/zdrowie-uroda/art43787701-mlode-pokolenie-nie-chce-sie-starzec-jak-rodzice-optymizacja-robi-furore

https://tropicieletalentow.pl/do-ktorego-pokolenia-nalezysz/

https://www.green-news.pl/4384-spor-o-nazwy-dla-miesa-roslinnego-w-unii-europejskiej
https://www.newspoint.pl/blog/raport-newspoint-pokolenia-w-polsce-i-potrzeba-monitorowania-ich-rosnacej-aktywnosci
https://www.wirtualnemedia.pl/jezykowe-konflikty miedzypokoleniowe,7177871409059969a
https://zpe.gov.pl/a/przeczytaj/DjmClE4ck
https://zwierciadlo.pl/psychologia/536676,1,kiedy-ja-bylam-w-twoim-wieku-konflikt-pokolen-czyli-jak-nie-zostac-dziadersem.read
Samardakiewicz-Kirol E., Torres K., *Wyjątkowi jak płatki śniegu*, https://zdalne.umlub.edu.pl/doc/dzjuml3/Wyjatkowi_jak_platki_sniegu.pdf

Zuzanna ŚCIBURA[1]

KONFLIKTY EKONOMICZNE MIĘDZY PRZEDSIĘBIORSTWAMI W WARUNKACH WSPÓŁCZESNEJ KONKURENCJI RYNKOWEJ W POLSCE

Celem rozdziału jest analiza zjawiska konfliktów ekonomicznych między przedsiębiorstwami funkcjonującymi w warunkach współczesnej konkurencji rynkowej w Polsce. W opracowaniu przedstawiono istotę omawianych sporów, wskazując na ich powszechność oraz złożony charakter wynikający ze sprzeczności interesów podmiotów gospodarczych. W dalszej części dokonano klasyfikacji form, jakie przybierają analizowane zjawiska, uwzględniając m.in. rywalizację cenową, spory kontraktowe, działania niezgodne z zasadami uczciwej konkurencji oraz konflikty o charakterze wizerunkowym. Przedstawiono również konsekwencje tych zjawisk, wskazując zarówno ich pozytywny wpływ, jak i negatywne skutki. W opracowaniu podkreślono znaczenie właściwego zarządzania sytuacjami konfliktowymi oraz rolę regulacji prawnych w ograniczaniu ich skali i skutków. Zwrócono uwagę na znaczenie instytucji nadzorczych oraz norm prawnych kształtujących zasady funkcjonowania rynku.

Słowa kluczowe: rywalizacja rynkowa, ograniczone zasoby, strategie przedsiębiorstw, innowacyjność, efektywność gospodarcza.

Wprowadzenie

Współczesna gospodarka rynkowa charakteryzuje się intensywną konkurencją pomiędzy przedsiębiorstwami działającymi w różnych sektorach gospodarki. Przedsiębiorstwa rywalizują między sobą o klientów, dostęp do zasobów, udział w rynku oraz możliwość osiągnięcia przewagi konkurencyjnej. W takich warunkach naturalnym zjawiskiem stają się konflikty ekonomiczne między podmiotami gospodarczymi[2]. Konflikty te mogą przyjmować różne formy, wynikać z wielu czynników, takich jak sprzeczność interesów ekonomicznych, ograniczona dostępność zasobów czy agresywne strategie konkurencyjne. Są zjawiskiem nieuniknionym, ponieważ przedsiębiorstwa dążą do maksymalizacji własnych korzyści

[1] Zuzanna Ścibura, studentka Politechniki Rzeszowskiej im. Ignacego Łukasiewicza, Koło Naukowe Polityki Bezpieczeństwa Państwa.

[2] I. Otola, *Procesy Zarządzania przedsiębiorstwami a konkurencyjność w warunkach zarażonego rynku*, seria Monografie, nr 270, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2013, s. 116.

ekonomicznych. W warunkach współczesnej konkurencji rynkowej konflikty te mogą mieć zarówno charakter bezpośredni jak i pośredni[3].

Konflikt jest zjawiskiem powszechnie występującym w różnych obszarach życia społecznego i gospodarczego. W ujęciu ogólnym oznacza on sytuację, w której co najmniej dwie strony dążą do realizacji sprzecznych celów, a działania jednej z nich utrudniają osiągnięcie zamierzeń drugiej[4].

Konflikt ekonomiczny między przedsiębiorstwami można zdefiniować jako sytuację, w której podmioty gospodarcze, działające na tym samym lub powiązanym rynku, podejmują działania prowadzące do sprzeczności interesów ekonomicznych. Konflikty te mogą dotyczyć zarówno bezpośredniej rywalizacji o klientów i udział w rynku, jak i pośrednich aspektów działalności, takich jak dostęp do zasobów, kanałów dystrybucji czy technologii[5].

Istotą konfliktów ekonomicznych jest przede wszystkim ograniczoność zasobów oraz konieczność dokonywania wyborów przez przedsiębiorstwa. W warunkach gospodarki rynkowej podmioty gospodarcze konkurują o te same dobra, takie jak kapitał, praca, surowce czy uwaga konsumentów. W sytuacji, gdy zasoby te są ograniczone, działania jednego przedsiębiorstwa mogą bezpośrednio wpływać na możliwości rozwoju innych podmiotów, co prowadzi do powstawania konfliktów[6].

W gospodarce rynkowej konflikty między przedsiębiorstwami wynikają z samej istoty konkurencji. Konflikty te mają często charakter strategiczny i długoterminowy. Nie ograniczają się one jedynie do pojedynczych zdarzeń, lecz mogą stanowić element długotrwałej rywalizacji konkurencyjnej. Przedsiębiorstwa podejmują różnorodne działania mające na celu wzmocnienie swojej pozycji rynkowej[7].

W literaturze przedmiotu wskazuje się, że konflikty ekonomiczne mogą mieć zarówno charakter jawny jak i ukryty. Konflikty jawne przejawiają się w bezpośrednich działaniach przedsiębiorstw takich jak spory sądowe, kampanie marketingowe skierowane przeciwko konkurencji czy agresywne strategie cenowe. Z kolei konflikty ukryte mogą polegać na subtelnych działaniach takich jak próby przejmowania klientów, budowanie przewagi technologicznej czy ograniczanie dostępu konkurentów do kluczowych zasobów[8].

---

[3] J. Woś, *Rynek i państwo w modelach współczesnej gospodarki rynkowej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2001, z. 4, Wydawnictwo Uniwersytetu Adama Mickiewicza w Poznaniu, s. 179.

[4] J. Mucha, *Konflikt i społeczeństwo: z problematyki konfliktu społecznego we współczesnych teoriach zachodnich*, PWN, Warszawa 1978, s. 10-11.

[5] A. Bomba, P.A. Kubisiak, *Wojna ekonomiczna i jej skutki społeczne*, „Zeszyty Naukowe WSOWL" 2012, nr 3(165), s. 57.

[6] D. Dymkowski, M. Jaroszyńska, *Teoria wojny ekonomicznej*, „Studia Bezpieczeństwa Narodowego" 2015, nr 7, s. 186.

[7] I. Salejko-Szyszczak, *Klasyfikacja konfliktów w przedsiębiorstwie*, „Zarządzanie" 2011, XXXVIII, z. 404, Wydawnictwo Uniwersytetu Mikołaja Kopernika, s. 141.

[8] Tamże, s. 138.

Złożony charakter tych konfliktów sprawia, że mogą one jednocześnie stanowić zagrożenie dla stabilności rynku, jak i czynnik stymulujący jego rozwój.

Przyczyny powstawania konfliktów ekonomicznych między przedsiębiorstwami

Powstawanie konfliktów ekonomicznych między przedsiębiorstwami jest zjawiskiem ściśle związanym z mechanizmem funkcjonowania gospodarki rynkowej. Przedsiębiorstwa nieustannie dążą do osiągania przewagi konkurencyjnej, zwiększania udziału w rynku oraz maksymalizacji efektów ekonomicznych swojej działalności. W rezultacie pojawiają się konflikty ekonomiczne, których źródła mają charakter zarówno rynkowy, organizacyjny, jak i instytucjonalny[9].

Jedną z podstawowych przyczyn powstawania tych konfliktów jest fakt, że przedsiębiorstwa posiadają ograniczone zasoby. Każde z nich, funkcjonując na rynku, zabiega o dostęp do określonych dóbr i czynników produkcji takich jak kapitał, surowce, wykwalifikowani pracownicy czy atrakcyjne kanały dystrybucji. Jednak zasoby te są ograniczone, a ich dostępność bywa uzależniona od sytuacji gospodarczej czy pozycji rynkowej danej firmy. W sytuacji gdy kilka podmiotów konkuruje o te same zasoby, naturalnie pojawia się napięcie, co może prowadzić do konfliktu[10].

Kolejną istotną przyczyną konfliktów ekonomicznych jest walka o klienta i udział w rynku. Współczesne firmy w dużej mierze opierają się na zdolności do przyciągania i utrzymywania konsumentów. Obecnie występuje duże nasycenie rynku, z tego więc względu przedsiębiorstwa są zmuszone do coraz bardziej intensywnej rywalizacji zarówno pod względem ceny, jakości jak i sposobu komunikacji marketingowej. W takich sytuacjach konflikt często nie wynika tylko z samej obecności wielu podmiotów na rynku, ale także z bezpośredniego zderzenia ich celów strategicznych[11].

Poszczególne podmioty gospodarcze mogą realizować odmienne cele, stosować inne modele biznesowe oraz przyjmować różne strategie rozwoju. W praktyce oznacza to, że działania jednego przedsiębiorstwa mogą pozostawać w sprzeczności z zamierzeniami drugiego. Występuje to zwłaszcza w sytuacji, gdy firmy funkcjonują w tej samej branży, ale różnią się skalą działalności, kapitałem czy zakresem przewagi konkurencyjnej. Tego rodzaju rozbieżności często prowadzą do

---

[9] W. Szymański, *Niestabilność światowych finansów – przyczyny i konsekwencje* [w:] *Funkcjonowanie podmiotów w na rynkach finansowych w warunkach zmian i niestabilności*, red. T.P. Tkaczyk, „Przedsiębiorczość i Zarządzanie" 2014, t. XV, z. 6, cz. II, Wydawnictwo Społecznej Akademii Nauk, Łódź, s. 1-2.

[10] M. Romanowska, *Planowanie strategiczne w przedsiębiorstwie*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2009, s. 230.

[11] M. Sławińska, *Handel we współczesnej gospodarce. Nowe wyzwania*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2016, s. 152.

sporów, zwłaszcza wtedy, gdy jeden z podmiotów zaczyna podejmować działania ograniczające możliwość rozwoju drugiego[12].

Szczególnie istotnym źródłem konfliktów ekonomicznych między przedsiębiorstwami jest konkurencja cenowa. Cena jest jednym z najważniejszych instrumentów walki rynkowej, dlatego przedsiębiorstwa często wykorzystują ją jako podstawowe narzędzie do zdobywania przewagi nad konkurentami. Obniżanie cen może być skuteczną metodą przyciągania klientów, jednak równocześnie może wywoływać reakcje innych podmiotów, które, chcąc utrzymać swoją pozycję, również decydują się na redukcję cen[13].

Przyczyną powstawania konfliktów ekonomicznych jest także rozwój nowych technologii oraz wdrażane innowacje. W nowoczesnej gospodarce przewaga poszczególnych firm coraz częściej opiera się na technologii, którą posiadają oraz na zdolności do tworzenia nowych rozwiązań. Przedsiębiorstwa inwestujące w badania i rozwój starają się chronić efekty swojej działalności poprzez patenty, znaki towarowe czy prawa autorskie. Jednocześnie na rynku pojawiają się sytuacje, w których dochodzi do sporów o naruszenie tych praw. Zdarzenia te są coraz częstsze, zwłaszcza w branżach opartych na innowacyjności i silnej identyfikacji marki[14].

Nie bez znaczenia pozostają także praktyki nieuczciwej konkurencji, które stanowią jedną z przyczyn sporów między przedsiębiorstwami. W realiach współczesnej gospodarki nie wszystkie podmioty przestrzegają uczciwej rywalizacji w ramach obowiązujących norm prawnych i etycznych. Część firm podejmuje działania, które naruszają zasady sprawiedliwej konkurencji, takie jak rozpowszechnianie nieprawdziwych informacji o konkurentach, wprowadzanie klientów w błąd czy utrudnianie innym podmiotom dostęp do rynku. Tego rodzaju zachowania nie tylko destabilizują relacje rynkowe, lecz także prowadzą do sporów o charakterze prawnym i wizerunkowym[15].

Rodzaje konfliktów ekonomicznych

Konflikty ekonomiczne między przedsiębiorstwami mogą przyjmować zróżnicowane formy w zależności od specyfiki rynku, pozycji konkurencyjnej

---

[12] M.K. Gątarska, *Źródła konfliktów występujące w organizacji*, „Ekonomia i Zarządzanie" 2016, nr 2(9), Wydawnictwo Państwowej Wyższej Szkoły Zawodowej, Włocławek, s. 3.

[13] M. Borys, *Zachowania przedsiębiorstw a kreowanie designu w warunkach strategicznego podejścia do kształtowania cen* [w:] *Zachowania rynkowe przedsiębiorstw w teorii i praktyce gospodarczej*, red. B. Majecka, M. Jarocka, Wydawnictwo Polskie Towarzystwo Ekonomiczne, Gdańsk 2015, s. 128-130.

[14] A. Becla, S. Czaja, *Wynikające z innowacji zagrożenia bezpieczeństwa informacyjnego w społeczeństwie informacyjnym i gospodarce opartej na wiedzy oraz ich konsekwencje ekonomiczne* [w:] *Innowacje w dobie technologii IT,* red. Z. Malara, M. Rutkowska, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2020, s. 57-58.

[15] M. Klawikowski, *Zachowania biur podróży wobec społeczno-gospodarczych przemian na świecie* [w:] *Zachowania rynkowe…,* dz. cyt., s. 49.

poszczególnych podmiotów czy obszaru, w którym dochodzi do zdarzenia interesów. Jednym z najbardziej typowych rodzajów konfliktów ekonomicznych są konflikty cenowe. Obniżenie cen produktów lub usług, jako podstawowe narzędzie walki konkurencyjnej, ma na celu zwiększenie atrakcyjności oferty i przyciągnięcie klientów. Jednak równocześnie może wywoływać reakcję konkurentów, którzy, chcąc utrzymać swoją pozycję rynkową, podejmują analogiczne działania. W konsekwencji dochodzi do eskalacji rywalizacji. Konflikty cenowe są szczególnie częste na rynkach o dużym nasyceniu podmiotów oraz w branżach, w których produkty są do siebie zbliżone a cena stanowi dla konsumenta główne kryterium wyboru[16].

Drugą istotną kategorię stanowią konflikty o klientów i udział w rynku. Przedsiębiorstwa nieustannie zabiegają o pozyskanie nowych odbiorców oraz utrzymanie lojalności już istniejących. Działania te obejmują m.in. agresywne kampanie promocyjne, programy lojalnościowe, rozwój nowych kanałów sprzedaży czy rozszerzanie oferty produktowej. Konflikt pojawia się wówczas, gdy działania jednej z firm prowadzą do przejmowania klientów konkurencji lub osłabienia jej pozycji w danym segmencie rynku. Konflikty tego rodzaju często mają charakter długotrwały, ponieważ podmioty gospodarcze stale rywalizują między sobą o preferencję konsumentów i starają się budować trwałą przewagę konkurencyjną[17].

Częstym przypadkiem są także konflikty związane z nieuczciwą konkurencją. Występują wtedy, gdy przedsiębiorstwo podejmuje działania wykraczające poza ramy uczciwej rywalizacji rynkowej. Mogą one obejmować m.in. rozpowszechnianie nieprawdziwych lub wprowadzających w błąd informacji o konkurencie, podszywanie się pod jego markę, naśladownictwo produktów czy utrudnianie innym podmiotom dostęp do rynku. W praktyce bardzo często tego rodzaju spory prowadzą do batalii sądowych, interwencji organów regulacyjnych oraz poważnych konkurencji wizerunkowych[18].

Warto również zwrócić uwagę na konflikty wizerunkowe i marketingowe, które we współczesnej gospodarce odgrywają coraz większą rolę. W warunkach silnej presji konkurencyjnej przedsiębiorstwa starają się budować rozpoznawalność marki oraz pozytywny wizerunek. Konflikty pojawiają się wtedy, gdy działania promocyjne jednego podmiotu bezpośrednio lub pośrednio uderzają w konkurenta, na przykład poprzez reklamę porównawczą czy sugestie obniżające wiarygodność innej firmy. W dobie mediów społecznościowych i szybkiego przepływu informacji konflikty wizerunkowe rozwijają się bardzo dyna-

[16] M. Romanowska, *Planowanie strategiczne…,* dz. cyt., s. 208.

[17] M. Berger, M. Mitręga, *Istota i konsekwencje konfliktu w relacjach między przedsiębiorstwem a klientem*, „Zeszyty Naukowe Wydziałowe Uniwersytetu Ekonomicznego w Katowicach. Studia Ekonomiczne" 2014, nr 182, s. 46-47.

[18] M. Romanowska, *Planowanie strategiczne…,* dz. cyt., s. 174-176.

micznie i mogą wywoływać skutki wykraczające poza tradycyjną sferę ekonomiczną[19].

Osobną kategorię stanowią konflikty kontraktowe**,** które wynikają z realizacji umów handlowych między przedsiębiorstwami. Mimo że relacje kontraktowe opierają się formalnie na współpracy, bardzo często stają się źródłem napięć i sporów. Przyczyną konfliktu może być niewywiązywanie się z warunków umowy, opóźnienia w dostawach, zmiana cen, różnice w interpretacji postanowień kontraktowych czy niewłaściwa jakość dostarczanych towarów i usług. Konflikty kontraktowe pokazują, że konflikt ekonomiczny może pojawiać się nie tylko między bezpośrednimi konkurentami, lecz także między partnerami biznesowymi[20].

W praktyce rynkowej można wskazać także konflikty wynikające z nadużywania pozycji rynkowej**.** Dotyczą sytuacji, w których przedsiębiorstwo posiadające silniejszą pozycję ekonomiczną lub dominującą rolę na rynku wykorzystuje swoją przewagę w sposób ograniczający możliwości działania innych podmiotów. Może to polegać na narzucaniu niekorzystnych warunków współpracy, stosowaniu praktyk dyskryminacyjnych lub wypieraniu konkurentów z rynku. Konflikty te są szczególnie istotne z punktu widzenia ochrony konkurencji, ponieważ mogą prowadzić do zachwiania równowagi rynkowej i osłabienia rozwoju mniejszych przedsiębiorstw. W warunkach polskich zagadnienie to jest szczególnie istotne w odniesieniu do relacji między dużymi sieciami handlowymi a mniejszymi dostawcami czy producentami[21].

Konflikty ekonomiczne między przedsiębiorstwami przybierają wiele różnych form. Ich występowanie jest naturalnym zjawiskiem, jednak skala i sposób przebiegu mają istotny wpływ na stabilność rynku, warunki konkurencji oraz możliwości rozwoju przedsiębiorstw.

Skutki konfliktów ekonomicznych dla przedsiębiorstw i rynku

Rozpatrując problem konfliktów ekonomicznych między przedsiębiorstwami, istotne jest uwzględnienie ich konsekwencji dla działalności podmiotów gospodarczych oraz dla mechanizmów rynkowych. Skutki tych zjawisk mogą być zróżnicowane i zależą od wielu czynników takich jak charakter konkurencji, specyfika branży czy przyjęte strategie działania przedsiębiorstw.

W pierwszej kolejności należy zwrócić uwagę na pozytywne skutki konfliktów ekonomicznych, które często są niedoceniane, a jednocześnie odgrywają

[19] M. Adamczyk, *Wizerunek rynkowy jako element zarządzania przedsiębiorstwem* [w:] *Wybrane aspekty skutecznego zarządzania*, „Zeszyty Naukowe Wydziału Zarządzania GWSH" 2020, nr 14, Wydawnictwo Arterior, Katowice, s. 12.

[20] K. Kalawska, *Konflikt interesów w organizacji – ryzyko prawne, reputacyjne i operacyjne*, https://grantthornton.pl/publikacja/konflikt-interesow-w-organizacji-ryzyko-prawne-reputacyjne-i-operacyjne/ (dostęp: 23.03.2026 r.).

[21] M. Romanowska, *Planowanie strategiczne…,* dz. cyt., s. 202-203.

ważną rolę w rozwoju gospodarki rynkowej. Jednym z najważniejszych efektów jest wzrost innowacyjności. Rywalizacja zmusza podmioty gospodarcze do poszukiwania nowych rozwiązań technologicznych, organizacyjnych oraz produktowych. Przedsiębiorstwa, chcąc utrzymać lub poprawić swoją pozycję, inwestują w badania i rozwój, wprowadzają nowe produkty na rynek oraz usprawniają istniejące procesy. W efekcie konflikty ekonomiczne mogą przyczyniać się do zwiększenia dynamiki rozwoju całych branż[22].

Pozytywnym skutkiem konfliktów niewątpliwie jest poprawa jakości produktów i usług. W warunkach silnej konkurencji przedsiębiorstwa dążą do wyróżnienia swojej oferty, co często prowadzi do podnoszenia standardów jakościowych, lepszego dostosowania produktów do potrzeb klientów oraz zwiększenia poziomu obsługi. Konsumenci stają się w takiej sytuacji beneficjentami konfliktów rynkowych, ponieważ mają dostęp do coraz bardziej zaawansowanych, funkcjonalnych i atrakcyjnych ofert[23].

Można także wskazać na kolejną korzyść dla konsumentów w postaci obniżenia cen. Rywalizacja cenowa sprawia, że konsumenci mają możliwość wyboru tańszych ofert, co wpływa na poprawę ich sytuacji ekonomicznej[24].

Istotnym aspektem jest również zwiększenie efektywności działania przedsiębiorstw. Konflikty ekonomiczne zmuszają firmy do optymalizacji kosztów, usprawniania procesów produkcyjnych i logistycznych oraz bardziej racjonalnego zarządzania zasobami. W dłuższej perspektywie procesy te sprzyjają usprawnianiu działalności przedsiębiorstw oraz ich zdolności adaptacyjnych w zmieniającym się otoczeniu rynkowym[25].

Konflikty ekonomiczne mogą także pełnić funkcję mechanizmu selekcyjnego na rynku. W wyniku intensywnej konkurencji słabsze lub mniej efektywne przedsiębiorstwa mogą zostać wyeliminowane z rynku, co prowadzi do jego uporządkowania i zwiększenia ogólnej efektywności. Pozostające na rynku podmioty są zazwyczaj lepiej przygotowane do funkcjonowania w wymagającym otoczeniu gospodarczym. Dzięki czemu rynek jest coraz doskonalszy[26].

Pomimo licznych pozytywnych aspektów, konflikty ekonomiczne niosą ze sobą również szereg negatywnych konsekwencji, które mogą wpływać destabilizująco na funkcjonowanie przedsiębiorstw oraz całego rynku. Jednym z najważniejszych negatywnych skutków są straty finansowe ponoszone przez przedsiębiorstwa. Intensywna rywalizacja, zwłaszcza w formie wojen cenowych, może

---

[22] Tamże, s. 213-214.

[23] Rozwiazkonflikt.pl, *Czy konflikty mogą być pozytywne? Jak sprzeczki napędzają rozwój firm*, https://rozwiazkonflikt.pl/czy-konflikty-moga-byc-pozytywne-jak-sprzeczki-napedzaja-rozwoj-firm/ (dostęp: 23.03.2026 r.).

[24] K. Zieliński, *Kształtowanie cen we współczesnej gospodarce*, Wydawnictwo Akademii Nauk Stosowanych w Nowym Sączu, Nowy Sącz 2025, s. 20.

[25] Tamże, s. 20-25.

[26] M. Gorynia, B. Jankowska, *Wpływ klasterów na konkurencyjność i internacjonalizację przedsiębiorstw*, „Gospodarka Narodowa" 2007, nr 7-8 (191-192), Wydawnictwo Szkoły Głównej Handlowej, Warszawa, s. 2-3.

prowadzić do znacznego obniżenia marż oraz pogorszenia wyników finansowych. Długotrwałe konflikty mogą w skrajnych przypadkach doprowadzić nawet do upadłości przedsiębiorstw[27].

Istotnym problemem jest także pogorszenie relacji biznesowych. Konflikty między przedsiębiorstwami mogą prowadzić do utraty zaufania, ograniczenia współpracy oraz zaostrzenia relacji między partnerami gospodarczymi. W praktyce może to skutkować zerwaniem kontraktów, trudnościami w negocjacjach czy ograniczeniem możliwości rozwoju wspólnych przedsięwzięć[28].

Negatywnym skutkiem konfliktów ekonomicznych jest także destabilizacja rynku. Nadmierna intensyfikacja rywalizacji, zwłaszcza w sektorach o dużym znaczeniu dla gospodarki, może prowadzić do zaburzenia równowagi rynkowej. Przykładem mogą być sytuacje, w których agresywna polityka cenowa powoduje spadek rentowności całej branży lub gdy dominujące przedsiębiorstwa eliminują konkurencję, prowadząc do ograniczenia różnorodności oferty rynkowej[29].

Znaczącym obciążeniem dla przedsiębiorstw pozostają również koszty związane z rozwiązywaniem konfliktów, obejmujące m.in. postępowania sądowe, obsługę prawną czy działania mediacyjne. Spory gospodarcze, szczególnie te dotyczące własności intelektualnej lub realizacji kontraktów, mają często charakter długotrwały i generują wysokie wydatki, co ogranicza możliwości inwestycyjne przedsiębiorstw[30].

Nie bez znaczenia pozostaje także wpływ konfliktów na wizerunek przedsiębiorstw. Publiczne spory, zarzuty związane z nieuczciwą konkurencją oraz nagłaśniane konflikty prawne mogą prowadzić do stopniowej utraty zaufania klientów i partnerów biznesowych. W warunkach dynamicznego przepływu informacji negatywny wizerunek przedsiębiorstwa rozprzestrzenia się w krótkim czasie, pogłębiając konsekwencje konfliktu[31].

W ujęciu makroekonomicznym konflikty mogą prowadzić do ograniczenia stabilności i przewidywalności otoczenia gospodarczego. Wysoki poziom napięć między przedsiębiorstwami może zniechęcać inwestorów oraz wpływać na ogólny poziom zaufania w gospodarce. Skutki konfliktów (lub same konflikty) z jednej strony stanowią istotny mechanizm napędzający rozwój gospodarczy, z drugiej jednak mogą prowadzić do strat finansowych oraz destabilizacji rynku[32].

---

[27] S. Flejterski, M. Zioło, *Intra- i intersektorowe konflikty interesów finansowych. W poszukiwaniu wstępu do teorii*, „Annales. Etyka w Życiu Gospodarczym" 2017, t. 51, nr 4, UMCS, s. 110-111.

[28] M. Pawłowska, *Metodyka rozwiązywania konfliktów w procesie sukcesji w polskich przedsiębiorstwach rodzinnych*, Poznań 2019, s. 37-38.

[29] Kantor-bielsko.pl, *Ekonomiczne skutki wojen i konfliktów*, https://kantor-bielsko.pl/ekonomiczne-skutki-wojen-i-konfliktow/ (dostęp: 24.03.2026 r.).

[30] K. Dębkowska, *Mniejsze obciążenia biurokratyczne szansą na rozwój polskich firm*, „Tygodnik Gospodarczy PIE", Wydawnictwo Polski Instytut Ekonomiczny, Warszawa 2025, s. 2-3.

[31] O. Gorbaniuk, E. Samardakiewicz, *Zarządzanie antykryzysowe a wizerunek firmy*, „Organizacja i Kierowanie" 2011, nr 4, Wydawnictwo Szkoły Głównej Handlowej, Warszawa, s. 81-83.

[32] K. Januszewska, T. Kulig, J. Olszowy, *Analiza dynamiki integracji i globalizacji w kontekście niepewności i ryzyka* [w:] *Symbioza teorii i praktyki: innowacje, perspektywy w ekonomii i finansach*, red. J. Olszowy, Wydawnictwo Naukowe Archaegraph, Łódź 2024, s. 15-43.

Rola zarządzania w ograniczaniu konfliktów ekonomicznych

Konflikty ekonomiczne między przedsiębiorstwami stanowią naturalny element funkcjonowania gospodarki rynkowej, jednak ich przebieg oraz konsekwencje w dużej mierze zależą od sposobu, w jaki podmioty gospodarcze nimi zarządzają. Odpowiednie podejście do konfliktów pozwala nie tylko ograniczać ich negatywne skutki, ale także wpływać na długookresowe funkcjonowanie przedsiębiorstw[33].

W tym kontekście szczególne znaczenie ma świadome kształtowanie strategii konkurencyjnych, które powinno opierać się na długofalowym podejściu do rozwoju przedsiębiorstwa. Strategia, zgodnie z ujęciem M.E. Portera, stanowi proces określania długofalowych celów przedsiębiorstwa oraz doboru odpowiednich działań i alokacji zasobów niezbędnych do ich realizacji. Orientacja na budowanie trwałej przewagi konkurencyjnej poprzez jakość, innowacyjność oraz rozwój oferty sprzyja ograniczaniu napięć i stabilizowaniu relacji między przedsiębiorstwami[34].

Istotna jest także komunikacja oraz jakość relacji między podmiotami gospodarczymi, które w wielu przypadkach decydują o przebiegu konfliktu. Trudności w wymianie informacji, brak przejrzystości działań czy różne interpretacje warunków współpracy mogą prowadzić do eskalacji sporów i nieporozumień, co jest ważnym aspektem zarówno w analizie strategicznej przedsiębiorstwa, jak i przy identyfikowaniu barier skutecznej strategii. W literaturze przedmiotu podkreśla się, że systematycznie prowadzony dialog, negocjacje oraz stosowanie mechanizmów mediacyjnych sprzyjają wczesnemu rozpoznawaniu i łagodzeniu konfliktów, zanim przyjmą one złożoną i kosztowną formę, co wpływa na efektywność realizacji strategii organizacji[35].

Ważnym elementem ograniczania konfliktów jest przestrzeganie zasad etyki biznesu, które wyznaczają ramy odpowiedzialnego funkcjonowania przedsiębiorstw na rynku. Działania zgodne z zasadami uczciwej konkurencji – takie jak rzetelne informowanie klientów, szacunek wobec partnerów biznesowych oraz unikanie działań naruszających interesy konkurentów – redukują ryzyko sporów wynikających z nieetycznych praktyk. Przestrzeganie etyki biznesu sprzyja budowaniu zaufania oraz stabilności relacji między uczestnikami rynku[36].

---

[33] Witalni.pl, *Zarządzanie konfliktem w firmie jako klucz efektywności i harmonii w zespole*, https://witalni.pl/baza_wiedzy/zarzadzanie-konfliktem-w-firmie-jako-klucz-do-efektywnosci-i-harmonii-w-zespole/ (dostęp: 25.03.2026 r.).

[34] M. Romanowska, *Planowanie strategiczne…,* dz. cyt., s. 16.

[35] A. Kozina, T. Małkus, A. Pieczonka, *Zasady mediacji w rozwiązywaniu konfliktów organizacyjnych w systemie logistycznym przedsiębiorstwa*, „Przegląd Organizacji" 2019, nr 11, Wydawnictwo Towarzystwo Naukowe Organizacji i Kierownictwa, s. 11-18.

[36] J. Korpysa, *Etyka biznesu. Studia przypadku*, Wydawnictwo Naukowe Uniwerystetu Szczecińskiego, Szczecin 2014, s. 11-16.

Oprócz przestrzegania zasad etyki biznesu, istotną rolę w ograniczaniu konfliktów odgrywa zarządzanie ryzykiem sporów, które stanowi integralny element systemu zarządzania przedsiębiorstwem. Proces ten obejmuje identyfikację potencjalnych źródeł konfliktów, ocenę ich możliwych konsekwencji oraz wdrażanie działań prewencyjnych, co pozwala zarówno ograniczyć prawdopodobieństwo wystąpienia sporów, jak i zredukować ich skalę. W praktyce działania te mogą obejmować m.in. precyzyjne konstruowanie umów, stosowanie procedur kontrolnych czy systematyczne monitorowanie relacji z partnerami biznesowymi[37].

Nie mniej istotna jest zdolność przedsiębiorstw do adaptacji w dynamicznie zmieniającym się otoczeniu rynkowym. Warunki rynkowe wymagają elastycznego reagowania na działania konkurencji oraz zmiany w otoczeniu gospodarczym. Przedsiębiorstwa, które skutecznie dostosowują swoje strategie i procesy operacyjne, są w stanie minimalizować napięcia oraz przeciwdziałać eskalacji konfliktów[38].

Rola regulacji prawnych w ograniczaniu konfliktów ekonomicznych

Funkcjonowanie przedsiębiorstw w gospodarce rynkowej wiąże się z przestrzeganiem określonych norm prawnych, które mają na celu zapewnienie równych warunków działania wszystkim uczestnikom rynku.

Z perspektywy omawianego zagadnienia pierwszorzędne znaczenie ma prawo konkurencji, którego podstawę w Polsce stanowi ustawa z dnia 16 lutego 2007 roku o ochronie konkurencji i konsumentów. Zgodnie z art. 6 tej ustawy zakazane są porozumienia między przedsiębiorstwami, których celem lub skutkiem jest ograniczenie konkurencji, w szczególności ustalanie cen czy podział rynku. Ponadto art. 9 wskazuje na zakaz nadużywania pozycji dominującej, co obejmuje m.in. narzucanie nieuczciwych cen lub warunków umów. Regulacje te ograniczają możliwość podejmowania działań prowadzących do eliminowania konkurencji, a tym samym zmniejszają ryzyko występowania konfliktów o charakterze ekonomicznym[39].

W związku z powyższym nie bez znaczenia pozostaje rola instytucji nadzorujących rynek, które czuwają nad przestrzeganiem obowiązujących przepisów oraz podejmują działania w przypadku ich naruszenia. W Polsce funkcję tę pełni przede wszystkim Urząd Ochrony Konkurencji i Konsumentów, który na podstawie art. 31 ustawy o ochronie konkurencji i konsumentów prowadzi postępowania

[37] Komisja Nadzoru Finansowego, *Obowiązki i odpowiedzialność organu zarządzającego*, https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/obowiazki_i_odpowiedzialnosc_organu_zarzadzajacego?articleId=90809&p_id=18 (dostęp: 25.03.2026 r.).

[38] M. Kraszewska, K. Pujer, *Konkurencyjność przedsiębiorstw. Sposoby budowania przewagi konkurencyjnej,* Wydawnictwo Exante, Wrocław 2017, s. 7.

[39] Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jedn. Dz.U. z 2025 r., poz. 1714 ze zm.).

w sprawach praktyk ograniczających konkurencję oraz może nakładać kary finansowe na przedsiębiorstwa naruszające przepisy. Działalność tych instytucji ma charakter zarówno kontrolny, jak i prewencyjny, ponieważ sama świadomość możliwości interwencji wpływa na zachowania przedsiębiorstw[40].

Ważną rolę odgrywają także mechanizmy rozwiązywania sporów przewidziane w systemie prawnym, które umożliwiają przedsiębiorstwom dochodzenie swoich praw w sposób uporządkowany. W tym zakresie szczególne znaczenie mają przepisy kodeksu cywilnego[41], w tym art. 353^1, który wskazuje na zasadę swobody umów, oraz art. 471, regulujący odpowiedzialność za niewykonanie lub nienależyte wykonanie zobowiązania. Przepisy te stanowią podstawę dochodzenia roszczeń w przypadku sporów kontraktowych między przedsiębiorstwami. Oprócz postępowań sądowych coraz większą rolę odgrywają również alternatywne metody rozwiązywania sporów, takie jak mediacja czy arbitraż.

Dodatkowo regulacje prawne pełnią funkcję zapobiegawczą, kształtując ramy funkcjonowania rynku i ograniczając możliwość występowania konfliktów jeszcze przed ich powstaniem. W tym kontekście istotne są przepisy dotyczące ochrony własności intelektualnej, w szczególności ustawa Prawo własności przemysłowej. Przykładowo art. 296 tej ustawy reguluje ochronę znaków towarowych, umożliwiając przedsiębiorstwom dochodzenie roszczeń w przypadku ich naruszenia. Jasno określone zasady ochrony praw wyłącznych zmniejszają ryzyko sporów oraz sprzyjają większej przejrzystości relacji gospodarczych[42].

Nie bez znaczenia pozostaje również rola sankcji prawnych, które stanowią istotny element systemu regulacyjnego. Zgodnie z art. 106 ustawy o ochronie konkurencji i konsumentów Prezes UOKiK może nałożyć na przedsiębiorstwo karę pieniężną za naruszenie przepisów dotyczących konkurencji. Przykładem praktycznego zastosowania tego mechanizmu jest decyzja Prezesa UOKiK dotycząca zmowy cenowej między przedsiębiorcami, w wyniku której na uczestników porozumienia nałożono milionowe kary finansowe, przekraczające 400 mln zł. Możliwość zastosowania sankcji finansowych działa odstraszająco i ogranicza skłonność przedsiębiorstw do podejmowania działań sprzecznych z prawem[43].

Podsumowanie

Konflikty ekonomiczne między przedsiębiorstwami stanowią nieodłączny element funkcjonowania gospodarki rynkowej. Z jednej strony mogą sprzyjać zwiększeniu dynamiki konkurencji oraz stymulować innowacyjność, z drugiej

[40] uokik.gov.pl, *Postępowania*, https://uokik.gov.pl/ograniczanie-konkurencji-postepowania (dostęp: 26.03.2026 r.).

[41] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (tekst jedn. Dz.U. z 2026 r., poz. 507).

[42] Ustawa z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej (tekst jedn. Dz.U. z 2023 r. poz. 1170 ze zm.).

[43] uokik.gov.pl, *Czysta energia i brudne praktyki. Prezes UOKiK nałożył ponad 7 mln zł kar na firmy z branży OZE*, https://uokik.gov.pl/czysta-energia-i-brudne-praktyki-prezes-uokik-nalozyl-ponad-7-mln-zl-kar-na-firmy-z-branzy-oze (dostęp: 26.03.2026 r.).

natomiast prowadzą do strat finansowych, destabilizacji rynku oraz pogorszenia relacji między podmiotami gospodarczymi. Ich ostateczny wpływ determinowany jest przede wszystkim przebiegiem oraz intensywnością danego konfliktu[44].

Ograniczanie negatywnych konsekwencji konfliktów wymaga skoordynowanego oddziaływania zarówno na poziomie przedsiębiorstw, jak i systemu prawnego. W tym zakresie istotne znaczenie ma świadome kształtowanie strategii konkurencyjnych, rozwijanie trwałych relacji biznesowych oraz respektowanie standardów etycznych. Równocześnie regulacje prawne, w szczególności z zakresu ochrony konkurencji, wraz z działalnością instytucji nadzorczych, wyznaczają ramy funkcjonowania rynku, sprzyjające utrzymaniu jego równowagi i przejrzystości[45].

W konsekwencji konflikty ekonomiczne nie powinny być ujmowane wyłącznie w kategoriach zjawiska negatywnego, lecz jako naturalny komponent mechanizmu rynkowego. Przy odpowiednim poziomie regulacji oraz racjonalnym zarządzaniu mogą one pełnić funkcję stymulującą rozwój gospodarczy. Niezbędne pozostaje jednak minimalizowanie ich destrukcyjnych skutków oraz zapewnienie warunków sprzyjających uczciwej, efektywnej i stabilnej konkurencji[46].

Bibliografia

Adamczyk M., *Wizerunek rynkowy jako element zarządzania przedsiębiorstwem* [w:] *Wybrane aspekty skutecznego zarządzania*, „Zeszyty Naukowe Wydziału Zarządzania GWSH" 2020, nr 14, Wydawnictwo Arterior, Katowice.

Becla A., Czaja S., *Wynikające z innowacji zagrożenia bezpieczeństwa informacyjnego w społeczeństwie informacyjnym i gospodarce opartej na wiedzy oraz ich konsekwencje ekonomiczne* [w:] *Innowacje w dobie technologii IT,* red. Z. Malara, M. Rutkowska, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2020

Berger M., Mitręga M., *Istota i konsekwencje konfliktu w relacjach między przedsiębiorstwem a klientem*, „Zeszyty Naukowe Wydziałowe Uniwersytetu Ekonomicznego w Katowicach. Studia Ekonomiczne" 2014, nr 182, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.

Bomba A., Kubisiak P.A., *Wojna ekonomiczna i jej skutki społeczne*, „Zeszyty Naukowe WSOWL" 2012, Wydawnictwo Akademii Wojsk Lądowych, nr 3(165), Wrocław.

Borys M., *Zachowania przedsiębiorstw a kreowanie designu w warunkach strategicznego podejścia do kształtowania cen* [w:] *Zachowania rynkowe przedsiębiorstw w teorii i praktyce*

[44] G. Łukasik, *Konflikty interesów w finansach przedsiębiorstwa (dyskusyjne problemy)*, „Studia Ekonomiczne. Zeszyty Naukowe" 2018, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, s. 62-63.

[45] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 oraz dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz. Urz. UE L 2024/2847 z 20.11.2024).

[46] W. Szymański, *Niestabilność światowych finansów – przyczyny i konsekwencje* [w:] *Funkcjonowanie podmiotów…,* dz. cyt., s. 1-2.

gospodarczej, red. B. Majecka, M. Jarocka, Wydawnictwo Polskie Towarzystwo Ekonomiczne, Gdańsk 2015.

Dębkowska K., *Mniejsze obciążenia biurokratyczne szansą na rozwój polskich firm*, „Tygodnik Gospodarczy PIE", Wydawnictwo Polski Instytut Ekonomiczny, Warszawa 2025.

Dymkowski D., Jaroszyńska M., *Teoria wojny ekonomicznej*, „Studia Bezpieczeństwa Narodowego" 2015, nr 7.

Flejterski S., Zioło M., *Intra- i intersektorowe konflikty interesów finansowych. W poszukiwaniu wstępu do teorii*, „Annales. Etyka w życiu gospodarczym" 2017, t. 51, nr 4, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin.

Gątarska M.K., *Źródła konfliktów występujące w organizacji*, „Ekonomia i Zarządzanie" 2016, nr 2(9), Wydawnictwo Państwowej Wyższej Szkoły Zawodowej, Włocławek, s. 3.

Gorbaniuk O., Samardakiewicz E., *Zarządzanie antykryzysowe a wizerunek firmy*, „Organizacja i Kierowanie" 2011, nr 4, Wydawnictwo Szkoły Głównej Handlowej, Warszawa.

Gorynia M., Jankowska B., *Wpływ klasterów na konkurencyjność i internacjonalizację przedsiębiorstw*, „Gospodarka Narodowa" 2007, nr 7-8, Wydawnictwo Szkoły Głównej Handlowej, Warszawa.

Januszewska K., Kulig T., Olszowy J., *Analiza dynamiki integracji i globalizacji w kontekście niepewności i ryzyka* [w:] *Symbioza teorii i praktyki: innowacje, perspektywy w ekonomii i finansach*, red. J. Olszowy, Wydawnictwo Naukowe Archaegraph, Łódź 2024.

Klawikowski M., *Zachowania biur podróży wobec społeczno-gospodarczych przemian na świecie* [w:] *Zachowania rynkowe przedsiębiorstw w teorii i praktyce gospodarczej*, red. B. Majecka, M. Jarocka, Wydawnictwo Polskie Towarzystwo Ekonomiczne, Gdańsk 2015.

Korpysa J., *Etyka biznesu. Studia przypadku*, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2014.

Kozina A., Małkus T., Pieczonka A., *Zasady mediacji w rozwiązywaniu konfliktów organizacyjnych w systemie logistycznym przedsiębiorstwa*, „Przegląd Organizacji" 2019, nr 11, Wydawnictwo Towarzystwo Naukowe Organizacji i Kierownictwa.

Kraszewska M., Pujer K., *Konkurencyjność przedsiębiorstw. Sposoby budowania przewagi konkurencyjnej,* Wydawnictwo Exante, Wrocław 2017.

Łukasik G., *Konflikty interesów w finansach przedsiębiorstwa (dyskusyjne problemy)*, „Studia Ekonomiczne. Zeszyty Naukowe" 2018, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.

Mucha J., *Konflikt i społeczeństwo: z problematyki konfliktu społecznego we współczesnych teoriach zachodnich*, PWN, Warszawa 1978.

Otola I., *Procesy zarządzania przedsiębiorstwami a konkurencyjność w warunkach zarażonego rynku*, seria Monografie, nr 270, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2013.

Pawłowska M., *Metodyka rozwiązywania konfliktów w procesie sukcesji w polskich przedsiębiorstwach rodzinnych*, Poznań 2019.

Romanowska M., *Planowanie strategiczne w przedsiębiorstwie*, PWE, Warszawa 2009.

Salejko-Szyszczak I., *Klasyfikacja konfliktów w przedsiębiorstwie*, „Zarządzanie" 2011, XXXVIII, z. 404, Wydawnictwo Uniwersytetu Mikołaja Kopernika.

Sławińska M., *Handel we współczesnej gospodarce. Nowe wyzwania*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2016.

Szymański W., *Niestabilność światowych finansów – przyczyny i konsekwencje* [w:] *Funkcjonowanie podmiotów na rynkach finansowych w warunkach zmian i niestabilności*, red. T.P.

Tkaczyk, „Przedsiębiorczość i Zarządzanie" 2014, t. XV, z. 6, cz. II, Wydawnictwo Społecznej Akademii Nauk, Łódź.

Woś J., *Rynek i państwo w modelach współczesnej gospodarki rynkowej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2001, z. 4, Wydawnictwo Uniwersytetu Adama Mickiewicza w Poznaniu.

Zieliński K., *Kształtowanie cen we współczesnej gospodarce*, Wydawnictwo Akademii Nauk Stosowanych w Nowym Sączu, Nowy Sącz 2025.

Prawodawstwo

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 oraz dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz. Urz. UE L 2024/2847 z 20.11.2024).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (tekst jedn. Dz.U. z 2026 r., poz. 507).

Ustawa z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej (tekst jedn. Dz.U. z 2023 r., poz. 1170 ze zm.).

Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jedn. Dz.U. z 2025 r., poz. 1714 ze zm.).

Netografia

Kalawska K., *Konflikt interesów w organizacji – ryzyko prawne, reputacyjne i operacyjne*, https://grantthornton.pl/publikacja/konflikt-interesow-w-organizacji-ryzyko-prawne-reputacyjne-i-operacyjne/

Kantor-bielsko.pl, *Ekonomiczne skutki wojen i konfliktów*, https://kantor-bielsko.pl/ekonomiczne-skutki-wojen-i-konfliktow/

Komisja Nadzoru Finansowego, *Obowiązki i odpowiedzialność organu zarządzającego*, https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/obowiazki_i_odpowiedzialnosc_organu_zarzadzajacego?articleId=90809&p_id=18

Rozwiazkonflikt.pl, *Czy konflikty mogą być pozytywne? Jak sprzeczki napędzają rozwój firm*, https://rozwiazkonflikt.pl/czy-konflikty-moga-byc-pozytywne-jak-sprzeczki-napedzaja-rozwoj-firm/

uokik.gov.pl, *Czysta energia i brudne praktyki. Prezes UOKiK nałożył ponad 7 mln zł kar na firmy z branży OZE*, https://uokik.gov.pl/czysta-energia-i-brudne-praktyki-prezes-uokik-nalozyl-ponad-7-mln-zl-kar-na-firmy-z-branzy-oze

uokik.gov.pl, *Postępowania*, https://uokik.gov.pl/ograniczanie-konkurencji-postepowania

Witalni.pl, *Zarządzanie konfliktem w firmie jako klucz efektywności i harmonii w zespole*, https://witalni.pl/baza_wiedzy/zarzadzanie-konfliktem-w-firmie-jako-klucz-do-efektywnosci-i-harmonii-w-zespole/

Piotr PADULA[1]

BEZPIECZEŃSTWO GRANIC PAŃSTWA W DOBIE KONFLIKTÓW HYBRYDOWYCH. PERSPEKTYWA INFORMACYJNA

Rozdział koncentruje się na analizie bezpieczeństwa granic państwowych w kontekście współczesnych konfliktów hybrydowych, ze szczególnym uwzględnieniem wymiaru informacyjnego. Przedstawione są zmieniające się uwarunkowania bezpieczeństwa oraz ograniczenia tradycyjnych metod ochrony granic wobec dynamicznie rozwijających się zagrożeń, które często przybierają formę działań niejednoznacznych prawnie i politycznie. Konflikty hybrydowe charakteryzują się złożoną strukturą oddziaływań, obejmującą zarówno działania militarne, jak i polityczne, ekonomiczne, prawne czy informacyjne, przy czym informacja staje się równorzędnym i niezwykle elastycznym narzędziem wpływu. Granica państwa funkcjonuje jako przestrzeń materialna, instytucjonalna i informacyjna, w której kumulują się działania hybrydowe, od presji migracyjnej po kampanie dezinformacyjne i manipulacje narracyjne. W pracy wskazano, że narracje dotyczące kryzysów granicznych w warstwie emocjonalnej mają wysoki potencjał polaryzujący, kształtując percepcję zagrożeń, legitymizację polityki państwa oraz poziom zaufania społecznego. Wnioski obejmują konieczność integracji instrumentarium informacyjnego z tradycyjnymi środkami ochrony granic, rozwój kompetencji informacyjnych społeczeństwa, spójność normatywną i proceduralną działań państwa oraz wprowadzenie mechanizmów uczenia się strategicznego. Skuteczność państwa w dobie konfliktów hybrydowych zależy od równoczesnego zarządzania bezpieczeństwem fizycznym, przepływem informacji i percepcją społeczną, co stanowi fundament budowy odporności narodowej.

Słowa kluczowe: granica państwowa, wymiar informacyjny, narracje kryzysowe, polaryzacja społeczna, percepcja zagrożeń, zarządzanie informacją.

Wprowadzenie

Niezwykle trudne zdaje się we współczesnym świecie jednoznaczne określenie, co wpływa na bezpieczeństwo, a co pozostaje czynnikiem neutralnym bądź sprzyjającym. Wszelkie struktury dążące do stworzenia ram przeciwdziałania zagrożeniom, które coraz częściej cechują się dynamiczną zmiennością, bez aktualizacji i adaptacji szybko stają się niewystarczające. Charakterystyka rzeczywistości podlega procesowi zmian, co jest naturalną właściwością. Kluczowe z punktu widzenia nauk o bezpieczeństwie staje się dostrzeżenie przeobrażania architektury dotychczasowych elementów powodujących stan zagrożenia czy szkodliwości zarówno na poziomie jednostki, a więc osobistym, organizacji, jak i państwa.

[1] Piotr Padula, student Politechniki Rzeszowskiej im. Ignacego Łukasiewicza, Koło Naukowe Polityki Bezpieczeństwa Państwa. ORCID: 0009-0004-8353-6675.

Podejmowanie działań w tej dziedzinie na poziomie monowizyjnie rozumianej rzeczywistości zamiast interdyscyplinarnego podejścia zdaje się istotnie pozostawać w konflikcie z realnym przebiegiem istoty[2]. Tradycyjnie pojmowane formy i rodzaje zagrożeń ewoluowały lub doszło do połączenia ich niektórych cech, tworząc nowe wyznawania, na które dotychczasowe środki stają się nieskuteczne. Zmiana postrzegania bezpieczeństwa bezprecedensowo ma także konotacje z rozwojem technologii i ich upowszechnieniem na skalę świata, wobec czego kształtują się także prekursorskie formy oddziaływania godzące w dobro człowieka, a także zbiorowości[3].

Granica państwowa jako współczesne środowisko bezpieczeństwa zarówno historycznie oraz w doktrynie politycznej ujmowana jest jako część terytorium, a więc elementu składowego definicji państwa[4]. Tradycyjne rozumienie granicy państwowej jako fizycznej linii oddzielającej terytoria stopniowo traci swoją analityczną wystarczalność. Zmiana paradygmatu prowadzenia konfliktów, a więc prowadzenie rywalizacji poniżej progu otwartej konfrontacji militarnej, warunkuje, iż granica coraz częściej staje się obszarem oddziaływań politycznych, migracyjnych, informacyjnych. W warunkach narastającej niestabilności międzynarodowej oraz rozwoju konfliktów hybrydowych bezpieczeństwo granic przestaje być wyłącznie domeną ochrony terytorialnej, a zyskuje wymiar funkcjonalny i informacyjny.

Charakterystyka prowadzonych konfliktów w XXI wieku uwydatnia odejście od tradycyjnego przekraczania granic państwa terytorialnie poprzez użycie sił zbrojnych. Nowy wymiar wyzwań na granicy to przede wszystkim działania w infosferze, zmiany regulacji prawnych, presja migracyjna czy oddziaływanie na społeczeństwo. W tym ujęciu należy zauważyć, że granica państwa staje się obszarem skumulowanego oddziaływania hybrydowego, w którym poszczególne elementy tworzą spójny mechanizm destabilizacji. W ujęciu niniejszego opracowania niezbędne jest stwierdzenie, że granica państwa stanowi dynamiczną przestrzeń konfliktu hybrydowego, w której zarządzanie informacją stanowi kluczowe narzędzie oddziaływania na bezpieczeństwo narodowe. Wskazane wydaje się zwrócenie uwagi na sposoby instrumentalizacji granic przez podmioty prowadzące działania hybrydowe, znaczenie informacji jako narzędzia presji oraz wpływ tych procesów na odporność państwa.

---

[2] Zob. M. Pomykała, *Bezpieczeństwo wewnętrzne państwa wobec współczesnych zagrożeń*, „Bezpieczeństwo. Teoria i Praktyka" 2009, nr 1-2, s. 33, 41.

[3] Zob. M. Jurgilewicz, *Bezpieczeństwo państwa a bezpieczeństwo jednostki*, „Modern Management Review" 2018, t. 23, nr 25(1), s. 51-52.

[4] Klasyczną trójelementową definicję państwa sformułował Georg Jellinek, wskazując, że państwo składa się z ludności, terytorium i suwerennej władzy zwierzchniej. Zob. G. Jellinek, *Allgemeine Staatslehre*, O. Häring, Berlin 1914, s. 58-70.
W prawie międzynarodowym podstawę konstytucyjną definiowania państwa stanowi Konwencja z Montevideo z 1933 r., która w art. 1 wymienia stałą ludność, określone terytorium (oddzielone granicą), rząd oraz zdolność do nawiązywania stosunków międzynarodowych. Zob. art. 1 Konwencji z Montevideo z dnia 26 grudnia 1933 r. (UNTS nr 165).

Konflikt hybrydowy – ujęcie teoretyczne

Współczesne uwarunkowania konfliktów są niezwykle różnorodne. Czynniki, które niegdyś nie były traktowane jako sposób oddziaływania, dziś stają się realnym środkiem służącym do osiągania zamierzonych celów. Wielość możliwości realizowania swojej polityki przez państwa, organizacje międzynarodowe, ugrupowania terrorystyczne czy zgromadzenia separatystyczne powoduje niezwykle wiele trudności w ocenie, czy dane działanie można zakwalifikować jako operację wpływu przewidzianą w prawie międzynarodowym, czy jako zupełnie nową metodę nieregulowaną jurysdykcyjnie, czy jest to swego rodzaju zjawisko wewnątrzspołeczne bez ingerencji zewnętrznego wpływu. Tak zarysowany stan rzeczy implikuje powstania nowego stylu prowadzenia konfliktów w XXI wieku[5], którego tak szerokie spektrum pól oddziaływania staje się ewaluacją sztuki wojennej[6]. W konsekwencji opisanych przemian coraz częściej podważa się aktualność klasycznych kategorii analitycznych służących do opisu konfliktów zbrojnych.

Tradycyjny, powszechnie funkcjonujący, podział na stan wojny i pokoju[7], działania militarne i niemilitarne[8], a także na aktorów państwowych i nie-

[5] O pojęciu wojny hybrydowej w literaturze wzmianki można zauważyć od końca XX wieku, ale rozwój myśli przypada na początek XXI wieku, co uwarunkowane jest rozwojem i upowszechnieniem nowych technologii, m.in. Internetu. Zob. A. Szczygielska, *Konflikt hybrydowy – analiza porównawcza źródeł wiedzy o zjawisku*, „Roczniki Nauk Społecznych" 2023, t. 15(51), nr 2, s. 36-39.

[6] Zob. Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 4, s. 39.

[7] Czas wojny i pokoju to pojęcia mające na celu w ujęciu tego opracowania wskazanie zmian w podejściu do prowadzenia konfliktów. Zob. M. Kołodziejczak, *Analiza pojęcia wojny, agresji i napaści zbrojnej oraz przykłady ich użycia w aktach prawnych obowiązujących w Rzeczypospolitej Polskiej*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2015, nr 2(14), s. 71-76. Czas wojny można określić jako „okres funkcjonowania państwa charakteryzujący się istnieniem ostrego konfliktu, w którym regulowanie sporów między zwaśnionymi (antagonistycznymi) stronami (państwami, blokami państw, narodami, grupami społecznymi) realizowane jest środkami przemocy (przy użyciu sił zbrojnych) w celu osiągnięcia określonych interesów politycznych, ekonomicznych, ideologicznych lub innych" – *Słownik terminów z zakresu bezpieczeństwa narodowego*, red. J. Kaczmarek, W. Łepkowski, B. Zdrodowski, AON, Warszawa 2008, s. 29.
Natomiast stan pokoju można określić „jako złożony i wieloaspektowy proces budowania oraz utrzymywania ładu, obejmujący zarówno wewnętrzną harmonię człowieka („pokój w ludziach"), jak i uwarunkowania społeczne, kulturowe, polityczne oraz relacje międzynarodowe i odpowiedzi na globalne wyzwania współczesnego świata" – A. Piejak, *Pomiędzy wojną i pokojem – przestrzeń budowania kultury pokoju* [w:] *Humanistyczne ambiwalencje globalizacji. Zbiór studiów*, red. A. Piejak, I. Wojnar, Warszawa 2021, s. 41.

[8] Działania militarne – zorganizowane przedsięwzięcia realizowane przez siły zbrojne państwa lub inne formacje zbrojne, wykorzystujące środki wojskowe w celu osiągnięcia celów politycznych, strategicznych lub operacyjnych. Obejmują one zarówno działania bojowe jak i odstraszanie, demonstrację siły, obronę terytorium, operacje pokojowe czy wsparcie sojusznicze.
Działania niemilitarne – celowe i skoordynowane przedsięwzięcia realizowane bez użycia sił zbrojnych, służące ochronie interesów państwa, osiąganiu celów strategicznych lub oddziaływaniu na

państwowych[9] okazuje się niewystarczający do uchwycenia charakteru współczesnych form rywalizacji[10]. W praktyce obserwuje się bowiem nakładanie się różnego rodzaju form presji, które pozostają poniżej progu otwartego konfliktu zbrojnego, jednocześnie wywierają realny i długofalowy wpływ na bezpieczeństwo państwa, często realizując niektóre znamiona tradycyjnie postrzeganego konfliktu, jednak nie na tyle czytelnie, by taką kategorią go objąć.

W odpowiedzi na te zjawiska i formy osiągania celów w literaturze naukowej coraz częściej stosowane jest pojęcie konfliktu hybrydowego, który w swej istocie odnosi się do specyficznego modelu prowadzenia działań konfrontacyjnych, w którym wykorzystana jest kombinacja adekwatnie skoordynowanych środków militarnych i pozamilitarnych. Kluczowe wydaje się jednak zauważenie, że trudno jednoznacznie sformułować, czym jest, a czym nie jest pojęcie hybrydowości, jak zauważa Monika Kwiecińska: „Wątpliwości budzi formułowanie nowych pojęć, np. wojna hybrydowa, konflikt hybrydowy, metody walki hybrydowej, zagrożenie hybrydowe. Zdolność sklasyfikowania czym jest hybrydowość w aspekcie militarnym jest niezwykle trudna, o ile zasadne jest w ogóle używanie tego sformułowania w tym obszarze”[11]. Konflikt hybrydowy w swym podstawowym założeniu, nie odrzuca historycznego dorobku polemologii, w tym idei i doktryn uprawiania wojny. Dotychczasowe klasyczne instrumenty siłowe zostają uzupełnione o narzędzia polityczne, informacyjne, ekonomiczne, prawne czy społeczne, stosowane w sposób zsynchronizowanych i adaptacyjny[12]. Konieczne wydaje się także wskazanie kilku podstawowych cech charakteryzujących pojęcie konfliktu hybrydowego, w celu zbudowania klarownej i uporządkowanej bazy pojęciowej.

---

inne podmioty poprzez środki polityczne, ekonomiczne, społeczne, informacyjne, dyplomatyczne, prawne lub cybernetyczne.
Zob. M. Kołodziejczak, *Definicyjno-prawne regulacje wojny oraz terminów pochodnych*, „Roczniki Nauk Prawnych” 2018, nr 28(4).

[9] Aktorzy państwowi – podmioty stosunków międzynarodowych posiadające suwerenność, określone terytorium, ludność oraz władzę zdolną do podejmowania decyzji i reprezentowania państwa na arenie międzynarodowej. Są podstawowymi uczestnikami systemu międzynarodowego, dysponującymi legalnym monopolem stosowania przymusu oraz zdolnością do zawierania umów, prowadzenia polityki zagranicznej i realizowania interesów narodowych. Do aktorów państwowych zalicza się przede wszystkim państwa oraz ich organy władzy.
Aktorzy niepaństwowi – podmioty funkcjonujące w środowisku krajowym lub międzynarodowym, które nie posiadają statusu suwerennego państwa, lecz wywierają wpływ na procesy polityczne, gospodarcze, społeczne i bezpieczeństwa. Mogą działać samodzielnie lub we współpracy z państwami. Do tej grupy zalicza się organizacje międzynarodowe, korporacje transnarodowe, organizacje pozarządowe, media, ruchy społeczne, grupy terrorystyczne czy podmioty cybernetyczne.

[10] Zob. A. Mumford, P. Carlucci, *Hybrid warfare: The continuation of ambiguity by other means*, „European Journal of International Security” 2023, nr 8.2, s. 198-199.

[11] M. Kwiecińska, *Nowy wymiar konfliktów zbrojnych: konflikt hybrydowy a konflikt pełzający*, „Doctrina Studia Społeczno-Polityczne” 2016, nr 13, s. 89.

[12] Zob. M. Banasik, R. Parafianowicz, *Teoria i praktyka działań hybrydowych*, „Zeszyty Naukowe AON” 2015, nr 2(99), s. 14.

Istotną cechą jest niejednoznaczność. Działania prowadzone w tym modelu rzadko przybierają formę otwartej agresji czy formalnie wypowiedzianej wojny, co utrudnia jednoznaczną kwalifikację prawną oraz opóźnia możliwość reakcji instrumentów państwa dotkniętego tego rodzaju oddziaływaniem. Brak jasno sprecyzowanego momentu rozpoczęcia konfliktu sprzyja stopniowej eskalacji napięcia, rozmycia granic między działaniami wrogimi a legalną aktywnością polityczną czy społeczną[13].

Kolejną charakterystyczną cechą konfliktów hybrydowych jest uznanie informacji za równorzędne narzędzie wywierania wpływu. Należy podkreślić, że współcześnie informacja przestaje pełnić funkcje jedynie rozpoznania, wsparcia operacji militarnych, a staje się samodzielnym instrumentem, w dodatku niezwykle plastycznym, niejednokrotnie z istotną luką kontrreakcji podmiotu atakowanego. Kontrola narracji, selektywna prezentacja faktów, dezinformacja, manipulacje emocjami społecznymi, profilowanie informacji pod odbiorcę podważa zaufanie do podmiotów państwowych oraz wpływa na procesy decyzyjne, bez konieczności wprowadzenia bezpośrednich sił militarnych[14].

Na uwagę zasługuje także zróżnicowanie aktorów zaangażowanych w konflikt hybrydowy oraz rozmycie ich przynależności. Obok państwa bardzo często występują podmioty niepaństwowe, struktury i związki paramilitarne, ugrupowania eksternistyczne, organizacje społeczne, a nawet podmioty formalnie niezależne, które działają jednak w sposób zbieżny z interesami określonego aktora strategicznego. Kluczowe zdaje się podkreślenie, że działania podejmowane przez podmioty wpływu nie mają charakteru jednorodnego i różnią się zarówno stopniem intencjonalności, jak i relacją do zamierzonych celów. Tutaj w sposób szczególny należy wyróżnić działania intencjonalnie ukierunkowane bezpośrednio na uzyskanie celu, a ich efekt jest również bezpośrednio powiązany z zamierzonym rezultatem, a także pośrednie, gdzie podjęte przedsięwzięcia nie są formalnie skierowane na cel strategiczny, jednak generują skutki sprzyjające jego osiągnięciu, tzw. rozmyta intencjonalność. Coraz częściej wykorzystywanym mechanizmem oddziaływania za pomocą szczególnie podmiotów niezależnych są operacje emergentne, gdzie nieplanowane wydarzenia zostają ukierunkowane i wykorzystane przez uczestnika konfliktu hybrydowego w ramach swojej strategii. Taka struktura „rozmytych" podmiotów wywierających wpływ komplikuje jednoznaczne przypisanie odpowiedzialności oraz sprzyja stosowaniu strategii zaprzeczania[15].

W rezultacie poprzez tak sformułowane pojęcie konfliktu hybrydowego naturalne wydaje się postrzeganie terminu nie jako odrębną kategorię konfliktu zbrojnego, lecz jako dynamiczny model prowadzenia rywalizacji, w którym kluczowe znaczenie należy przypisać elastyczności używanych narzędzi, wielopłaszczy-

[13] Zob. P. Ochmann, *Prawne implikacje wybranych elementów terminu „wojna hybrydowa"*, „Studia Prawa Publicznego" 2019, nr 4(28), s. 136-140.

[14] Tamże, s. 135.

[15] Zob. K. Grabkowska, *Próba wyjaśnienia pojęcia i istoty wojen hybrydowych*, „Świat Idei i Polityki" 2022, nr 14, s. 277.

znowemu oddziaływaniu oraz niejednokrotnie adaptacyjnemu podejściu oraz niejednoznaczności liczby stron zaangażowanych. Kształtowania konfliktu hybrydowego nie należy pojmować jako zamknięty zbiór cech, wraz z postępem nauki, myśli i technologii będzie się zmieniał, pewne właściwości będą zanikać, zaś inne pojawią się.

Granica państwa jako obszar konfliktu hybrydowego

Określenie własnego terytorium nie jest domeną współczesności, jest konstruktem, który jest powiązany od wielu stuleci z człowiekiem, aczkolwiek nie tylko. Podstawową zależnością granic stała się ich dwustronność, przez co należy rozumieć fakt, że gdzie kończy się terytorium jednego podmiotu, zaczyna się terytorium drugiego[16]. Pierwotne znaczenie granic państw obejmowało przede wszystkim te w obrębie lądu, wraz z postępem świata to pojęcie ewoluowało i współcześnie do podstawowych płaszczyzn granic państwa możemy zaliczyć oprócz lądowych także wodne, powietrzne, powierzchnię podziemną oraz coraz częściej cyberprzestrzeń. Terytorium państwa określone jest granicą, wyznacza ona położenie geograficzne, obszar zwierzchności i zakres władztwa państwowego.[17] W tych warunkach właściwe staje się podkreślenie znaczenia obrony granic, jest to pojęcie, które swoją użyteczność czerpie bezpośrednio z rywalizacji państw czy podmiotów o terytorium.

Należy zauważyć, że współczesne środowisko bezpieczeństwa ulega dynamicznym przeobrażeniom, w których tradycyjne rozumienie granicy państwowej jako fizycznej linii oddzielającej terytoria stopniowo traci swoją analityczną wystarczalność. W epoce złożonych konfrontacji poniżej progu wojny granica staje się również dynamicznym interfejsem informacyjnym[18]. Należy zatem podkreślić, że staje się miejscem produkcji i walidacji znaczeń sygnały (fakty, narracje, obrazy, ruchy ludności) przechodzą przez zestaw kanałów komunikacyjnych i interpretacyjnych, gdzie ich znaczenie jest redystrybuowane, kontekstualizowane oraz niejednokrotnie instrumentalizowane.

Zmiana perspektywy z postrzegania granicy jako bariery na traktowanie jej jako przestrzeni oddziaływań informacyjnych pozwala uchwycić specyfikę konfliktów hybrydowych. Granica staje się obszarem testowania zdolności państwa do reagowania na presję o niejednoznacznym charakterze, trudną do bezprocesowego zakwalifikowania w ujęciu prawnym i politycznym[19].

---

[16] Zob. P. Lubiewski, *Granice Rzeczypospolitej Polskiej jako wyzwanie dla bezpieczeństwa państwa*, „Przegląd Policyjny" 2019, nr 0 (specjalny), s. 50.

[17] Zob. G. Balawajder, *Granica państwa jako kategoria wielowymiarowa*, „Pogranicze. Polish Borderlands Studies" 2013, nr 1, s. 44-50.

[18] Zob. J. Kurczewska, *Granica niejedno ma imię. Trzy podejścia teoretyczne* [w:] *Granice na pograniczach*, red. J. Kurczewska, H. Bojar, Wydawnictwo IFiS PAN, Warszawa 2005, s. 368-369.

[19] Zob. J. Pettersson, *What's in a Line? Making Sovereignty through Border Policy*, PhD Thesis, "Acta Universitatis Upsaliensis" 2018, s. 22, 72.

Z perspektywy analitycznej granica państwowa może być ujmowana jako struktura wielowymiarowa, obejmująca co najmniej trzy współzależne warstwy:

1. materialno-logistyczna (infrastruktura, przepływ osób i towarów),
2. informacyjno-komunikacyjna (kanały przekazu, aktorzy medialni, sieci społecznościowe),
3. instytucjonalno-prawna (normy, procedury, przepisy, mechanizmy odpowiedzialności)[20].

Konflikt hybrydowy wykorzystuje napięcie i nieciągłości między tymi warstwami, eskalując presję w sposób stopniowy i trudny do jednoznacznego rozpoznania. Takie ujęcie implikuje konieczność redefinicji podejścia do bezpieczeństwa granic. Polityka ochrony granic musi integrować instrumentarium informacyjne z narzędziami tradycyjnej kontroli terytorialnej, nie jako dodatek, lecz jako współzależny komponent systemu bezpieczeństwa[21]. Równocześnie badania nad bezpieczeństwem granic w celu przeciwdziałania zagrożeniom hybrydowym powinny opierać się na metodach mieszanych: od sieciowej analizy przepływów narracyjnych, przez etnograficzne badania percepcji społeczności lokalnych, po ocenę proceduralną mechanizmów prawnych i ich punktów podatności. Przyjęcie takiego podejścia pozwala przesunąć dyskurs z deklaratywnego alarmu nad „hybrydowością" ku precyzyjnej analizie mechanizmów, które można mierzyć, modelować i w oparciu o wypracowane postulaty projektować polityki odpornościowe.

Wymiar informacyjny

Szczególną cechą wielu domen bezpieczeństwa wobec powszechnego dostępu do Internetu oraz technologii szybkiego rozpropagowywania informacji staje się konieczność oddziaływania właśnie w tej przestrzeni. Obszar granic państwa w rozumieniu procedur i działań podejmowanych w tej przestrzeni nie stanowi wyjątku. Współczesne konflikty hybrydowe cechują się przenikaniem wielu sektorów m.in.: militarnego, politycznego, ekonomicznego i właśnie informacyjnego[22]. Warto więc podkreślić, że granic państwowa w tym układzie staje się nie tylko przestrzeni fizycznej kontroli przepływów, lecz także obszarem intensywnych oddziaływań narracyjnych. Wymiar informacyjny konfliktów osadzonych w meritum strefy przygranicza ma charakter strategiczny, gdyż wpływa na percepcję zagrożeń, ocenę legalności działań państwa oraz poziom zaufania społecznego

[20] Zob. M. Więckowski, *Od barier i izolacji do sieci i przestrzeni transgranicznej – konceptualizacja cyklu funkcjonowania granic państwowych*, „Przegląd Geograficzny" 2019, nr 91.4, s. 449-450.

[21] Zob. Y. Likhovitskyy, P. Polián, N. Svyrydiuk, *Information Threats in the Context of Hybrid War*, „Advances in Economics, Business and Management Research" 2021, nr 188, s. 114.

[22] Zob. A.M. Dyner, *Kryzys graniczny jako przykład działań hybrydowych*, „PISM Strategic File" 2022, nr 2(110), s. 3.

do instytucji odpowiedzialnych za bezpieczeństwo[23]. Granica staje się tym samym przestrzenią konfrontacji nie tylko interesów, lecz także interpretacji.

Paradoksem oddziaływania hybrydowego jest fakt, że fizycznie nie wszystko dzieje się na granicy. Należy zauważyć, że wymiar informacyjny w gruncie rzeczy odnosi się do struktur danych przekazywanych społeczeństwom. Dokładnie tutaj urzeczywistnia się model działań pośrednich i emergentnych. Granica państwa posiada silny wymiar symboliczny, w wymiarze społecznym stanowi istotny element tożsamości zbiorowej i poczucia bezpieczeństwa. Z tego względu wszelkie zdarzenia zachodzące w przestrzeni granicznej łatwo podlegają symbolizacji i stają się nośnikiem znaczeń wykraczających poza ich bezpośredni, materialny charakter. Poprzez informacje zmanipulowane a zarazem zaakceptowane możliwe jest bowiem wpływanie na działania społeczne niekorzystne z punktu widzenia państwa[24]. Technik wpływania jest niezwykle wiele i nie sposób wymienić je wszystkie, gdyż ich katalog ciągle się zmienia i nie pozostaje usystematyzowany. Należy jednak wskazać narracje jako obszar pojęciowy, mieszczący wiele czynników kształtujących informacyjny wymiar bezpieczeństwa. Narracje dotyczące domniemanego lub faktycznego kryzysu na granicy w swojej warstwie emocjonalnej posiadają wysoki potencjał polaryzujący[25]. Konstrukcja powstałego przekazu może prowadzić do przedstawienia sytuacji w obszarze granic jako zagrożenia egzystencjalnego wymagającego nadzwyczajnych środków, bądź przeciwnie jako problemu humanitarnego wymagającego liberalizacji polityki państwa. Tego rodzaju dychotomiczne ramy interpretacyjne sprzyjają powstawaniu silnych podziałów społecznych, redukując przestrzeń dla zniuansowanej debaty publicznej. W rezultacie granica przestaje być wyłącznie przedmiotem polityki bezpieczeństwa, a staje się osią sporów ideowych.

Informacja odgrywa w tym procesie rolę czynnika kształtującego postawy społeczne. Selektywny dobór faktów, sposób ich prezentacji oraz kontekstualizacja zdarzeń wpływa na poziom akceptacji działań podejmowanych przez państwo[26]. Legitymizacja polityki granicznej nie jest bowiem wyłącznie konsekwencją jej skuteczności operacyjnej, lecz również efektem społecznej percepcji jej adekwatności i proporcjonalności. W warunkach konfliktu hybrydowego oddziaływanie na tę percepcję staje się kluczowym instrumentem destabilizacji, wynika to z podważenia zaufania obywateli do instytucji ochrony granic co może

[23] Zob. D. Kaźmierczak, M. Laskowski, *Social cohesion in hybrid conflicts. Case of migration crisis at the polish-belarussian border and migration flows from Ukraine*, „Przegląd Wschodnioeuropejski" 2024, nr 15.2, s. 114.

[24] Zob. J. Kossecki, *Proces produkcji informacji i jego wpływ na aktywność społeczną,* „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1973, nr 4, s. 215, 219-222.

[25] Zob. M. Filipiak, *Topiczna architektura platform internetowych a społeczna polaryzacja światopoglądowa*, „Journal of Modern Science" 2025, nr 3(63), s. 1047-1048.

[26] Zob. M. Palczewski, *Selekcja informacji w mediach – zasady, wartości, manipulacje*, „Naukowy Przegląd Dziennikarski" 2015, nr 2, s. 85-88.

prowadzić do erozji spójności wewnętrznej państwa[27]. Kluczowe jest założenie, że narracje to nie tylko domena podmiotów wpływających w swym założeniu na osiągnięcie celów poprzez destabilizację granicy jako efekt pośredni bądź końcowy. Takie działania nie muszą być wpływem zewnętrznym, może to być także rezultat grup wewnętrznych, chcących w ten sposób zrealizować swoje potrzeby. W konsekwencji granica funkcjonuje także jako przestrzeń produkcji narracji konkurencyjnych, w których ścierają się interpretacje dotyczące bezpieczeństwa, praw człowieka, suwerenności czy solidarności międzynarodowej. Intensywność tych sporów dowodzi, że w warunkach konfliktu hybrydowego kontrola nad przekazem informacyjnym staje się równie istotna jak kontrola nad samym terytorium.

Wymiar informacyjny konfliktów hybrydowych nie ogranicza się jedynie do rywalizacji narracyjnej o charakterze otwartym. Istotnym elementem pozostają działania dezinformacyjne oraz operacje wpływu, których celem ponownie jest osłabienie zaufania do instytucji państwowych oraz wywołanie poczucia chaosu decyzyjnego[28]. Dezinformacja niejednokrotnie przybiera formę fałszywych doniesień o działaniach służb, manipulacji obrazem sytuacji humanitarnej czy rozpowszechniania niezweryfikowanych informacji o rzekomych naruszeniach prawa. Nawet jeśli pojedyncze przekazy zostaną zdementowane, ich kumulatywny efekt może prowadzić do utrwalenia w społeczeństwie przekonania o nieporadności, niespójności lub niekompetencji aparatu państwowego. Manipulacja informacją może przyjąć formę nie tylko dezinformacji, ale także misinformacji[29] jak i malinfomacji. O ile pierwsza ze wspomnianych form tworzona jest intencjonalnie i dotyczy nieprawdziwych sytuacji, wydarzeń, informacji tak malinformacja wskazuje, że informacja, pomimo iż jest prawdziwa może zostać przedstawiona w takich okolicznościach, tle, sytuacji by była szkodliwa[30].

Szczególną rolę w tym procesie odgrywają media społecznościowe, które umożliwiają szybkie rozpowszechnianie treści nacechowanych emocjonalnie. Algorytmiczne wzmacnianie przekazów budzących silne reakcje sprzyja eskalacji napięć i utrudnia racjonalną ocenę sytuacji. Konflikty informacyjne w przestrzeni granicznej często opierają się na obrazach i relacjach o wysokim ładunku emocjonalnym, które są następnie wykorzystywane do budowania uproszczonych, spolaryzowanych narracji. Mechanizm ten zwiększa podatność społeczeństwa na manipulację oraz sprzyja radykalizacji stanowisk[31].

---

[27] Zob. D. Tomal, *Wiarygodność jako argument legitymizacyjny lokalnych przywódców politycznych*, rozprawa doktorska UKEN, Kraków 2025, s. 27-32.

[28] Zob. T. Kacała, *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2(24), s. 52, 54-55.

[29] Zob. I. Grabowska-Lepczak, B. Szykuła-Piec, J. Wasiluk, *Dezinformacja jako jedno z narzędzi w wojnie hybrydowej*, „Central European Journal of Security Studies" 2024, t. 2, nr 1, s. 10-12.

[30] Zob. W. Babik, *O manipulowaniu informacją w prywatnej i publicznej przestrzeni informacyjnej* [w:] *Człowiek, media, edukacja*, red. E. Musiał, I. Pilak, Kraków 2011, s. 13-15.

[31] Zob. K. Stankiewicz, *Wpływ Internetu na percepcje wiarygodności informacji* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?,* red. L. Haber, t. II, Kraków 2004, s. 408-414.

Dodatkowym czynnikiem wzmacniającym skuteczność operacji wpływu jest brak spójnej i konsekwentnej narracji państwowej. Niejednoznaczne komunikaty, opóźnienia informacyjne czy sprzeczne wypowiedzi przedstawicieli władz mogą tworzyć próżnię interpretacyjną, w której łatwo rozprzestrzeniają się alternatywne, często wrogie przekazy. W warunkach konfliktu hybrydowego spójność komunikacyjna stanowi zatem element odporności państwa, analogiczny do spójności instytucjonalnej czy operacyjnej. Kluczowe staje się, aby to komunikat państwowy wyprzedzał obce narracje oraz aby nie został przez nie zagłuszony[32].

Dezinformacja w obszarach przygranicznych ma wymiar strategiczny, ponieważ oddziałuje równocześnie na kilka poziomów: percepcję społeczną, legitymizację polityki państwa oraz jego wizerunek w środowisku międzynarodowym. Osłabienie któregokolwiek z tych elementów może ograniczyć zdolność państwa do skutecznego reagowania na presję hybrydową. Tym samym wymiar informacyjny konfliktów prowadzonych na granicach należy traktować jako integralny komponent bezpieczeństwa narodowego, wymagający systemowych rozwiązań w zakresie komunikacji strategicznej, budowy odporności społecznej oraz koordynacji międzyinstytucjonalnej.

Podsumowanie i rekomendacje

Przeprowadzona analiza prowadzi do wniosku, że współczesne bezpieczeństwo granic nie może być rozpatrywane wyłącznie w kategoriach kontroli terytorialnej ani jako domena wyłącznie operacyjna. Konflikty hybrydowe redefiniują funkcję granicy państwowej, czyniąc z niej przestrzeń wielowymiarowej rywalizacji, w której komponent informacyjny odgrywa rolę równorzędną wobec elementów materialnych i instytucjonalnych. Granica przestaje być wyłącznie linią oddzielającą porządki prawne i terytoria, a staje się dynamicznym polem oddziaływań narracyjnych, w którym rozstrzygają się kwestie legitymizacji, percepcji zagrożeń oraz spójności społecznej. W warunkach konfliktu hybrydowego fizyczne naruszenie granicy nie stanowi koniecznego warunku destabilizacji państwa. Wystarczające może okazać się oddziaływanie na sposób interpretacji wydarzeń, podważenie zaufania do instytucji ochrony granic czy wykreowanie wrażenia chaosu decyzyjnego. Oznacza to, że bezpieczeństwo granic należy ujmować jako kategorię systemową, obejmującą zarówno zdolności operacyjne, jak i kompetencje komunikacyjne oraz odporność społeczną. Państwo, które koncentruje się wyłącznie na wymiarze infrastrukturalnym, pozostaje podatne na działania wpływu prowadzone w przestrzeni informacyjnej[33]. Z perspektywy teoretycznej granica w dobie

[32] Zob. M. Kożdoń-Dębecka, *Polaryzacja medialna na przykładzie kryzysu migracyjnego na granicy polsko-białoruskiej latem 2021 roku w relacjach trzech polskich telewizyjnych serwisów informacyjnych*, „Media Biznes Kultura" 2023, nr 1(14), s. 171-172.

[33] Zob. A. Skwarski, P. Szkudlarek, *Rola informacji i zagrożenia dezinformacją w systemie bezpieczeństwa państwa*, „Studia Administracji i Bezpieczeństwa" 2020, nr 5, s. 24-26.

konfliktów hybrydowych funkcjonuje jako punkt koncentracji napięć pomiędzy trzema warstwami: materialno-logistyczną, informacyjno-komunikacyjną oraz instytucjonalno-prawną. Destabilizacja może następować nie poprzez bezpośrednie przełamanie którejkolwiek z nich, lecz poprzez wykorzystanie ich niespójności. W tym sensie wymiar informacyjny pełni funkcję katalizatora, wzmacniając istniejące napięcia i przekształcając incydenty o ograniczonym znaczeniu operacyjnym w kryzysy o wymiarze strategicznym.

W świetle powyższych ustaleń zasadne jest sformułowanie kilku kluczowych rekomendacji z punktu widzenia państwa. Po pierwsze, konieczna jest instytucjonalna integracja ochrony granic z systemem komunikacji strategicznej. Oznacza to, że działania operacyjne służb granicznych powinny być równolegle wspierane przez spójną, przewidywalną i proaktywną politykę informacyjną. Komunikat państwowy nie może mieć charakteru reaktywnego ani fragmentarycznego, powinien uprzedzać potencjalne narracje destabilizacyjne oraz minimalizować przestrzeń dla manipulacji. Po drugie, państwo powinno rozwijać zdolności w zakresie monitorowania i analizy środowiska informacyjnego wokół tematów przygranicznych. Nie chodzi wyłącznie o reagowanie na dezinformację, lecz o systemowe badanie trendów narracyjnych, identyfikację wzorców eskalacji emocjonalnej oraz analizę podatności społecznych. Wymaga to łączenia kompetencji służb bezpieczeństwa, ośrodków analitycznych oraz środowiska akademickiego.

Warto również podkreślić, że istotnym elementem odporności staje się budowa kompetencji informacyjnych społeczeństwa. Edukacja w zakresie rozpoznawania manipulacji, świadomości procesów dezinformacyjnych oraz rozumienia mechanizmów konfliktów hybrydowych powinna być traktowana jako komponent polityki bezpieczeństwa, a nie wyłącznie jako zadanie systemu edukacji. Społeczeństwo świadome mechanizmów wpływu stanowi bufor ochronny wobec operacji destabilizacyjnych. Komponentem konfliktu hybrydowego są działania ukierunkowane na nadanie informacjom konkretnych znaczeń oddziałujących na społeczeństwo, nauka więc weryfikacji informacji oraz myślenia strategicznego staje się nie tyle przyszłością co realnym wyzwaniem teraźniejszości.

Niezbędne staje się także wzmocnienie spójności normatywnej i proceduralnej działań państwa na granicy. Transparentność, przewidywalność oraz zgodność z prawem międzynarodowym ograniczają przestrzeń dla narracji delegitymizujących. W warunkach konfliktu hybrydowego każde działanie operacyjne posiada potencjalny wymiar informacyjny, dlatego projektowanie procedur powinno uwzględniać ich możliwe konsekwencje percepcyjne. Kluczowe staje się formułowanie praw tak, by realnie wspierały potencjał obronny. Potencjalne luki prawne, mogą prowadzić bowiem do ograniczania możliwości reagowania służb, jurysdykcja, więc powinna kształtować normy w taki sposób, aby jasno spełniały cel w jakim zostają wprowadzane, przy jednoczesnym przedziale swobody w ramach, której to podmiot reagowania ma możliwość doboru adekwatnych środków. Reagowanie państwa na informacyjny wymiar konfliktów hybrydowych na granicach powinno opierać się na zinstytucjonalizowanym mechanizmie uczenia się

strategicznego, obejmującym systematyczną analizę doświadczeń innych państw dotkniętych presją hybrydową oraz włączanie wniosków z tych analiz do krajowych dokumentów doktrynalnych, procedur operacyjnych i praktyk komunikacyjnych. Transnarodowy charakter operacji wpływu oraz powtarzalność ich schematów, adaptowanych do lokalnych uwarunkowań, uzasadniają konieczność porównawczej refleksji strategicznej jako stałego komponentu planowania bezpieczeństwa. Ochrona granic w wymiarze informacyjnym powinna być ujmowana jako proces ciągły, podlegający regularnej ewaluacji, aktualizacji i korekcie, co stanowi warunek utrzymania długofalowej odporności państwa na destabilizację hybrydową.

Podsumowując, bezpieczeństwo granic w dobie konfliktów hybrydowych wymaga odejścia od redukcjonistycznego podejścia opartego wyłącznie na kontroli fizycznej. Granica stanowi dziś jednocześnie przestrzeń operacyjną, symboliczną i informacyjną. Skuteczność państwa w tej sferze zależy nie tylko od zdolności do fizycznej ochrony terytorium, lecz również od umiejętności zarządzania znaczeniem, percepcją i zaufaniem społecznym. Wymiar informacyjny nie jest dodatkiem do bezpieczeństwa granic, stanowi jego integralny i strukturalny komponent. Odpowiedź państwa powinna mieć charakter systemowy, interdyscyplinarny i długofalowy, uwzględniający zarówno zmienność środowiska bezpieczeństwa, jak i ewolucję technologicznych form oddziaływania.

Bibliografia

Babik W., *O manipulowaniu informacją w prywatnej i publicznej przestrzeni informacyjnej* [w:] *Człowiek, media, edukacja*, red. E. Musiał, I. Pilak, Kraków 2011.

Balawajder G., *Granica państwa jako kategoria wielowymiarowa*, „Pogranicze. Polish Borderlands Studies" 2013, nr 1.

Banasik M., Parafianowicz R., *Teoria i praktyka działań hybrydowych*, „Zeszyty Naukowe AON" 2015, nr 2(99).

Carlucci P., Mumford A., *Hybrid warfare: The continuation of ambiguity by other means*, „European Journal of International Security" 2023, nr 8.2.

Dyner A.M., *Kryzys graniczny jako przykład działań hybrydowych*, „PISM Strategic File" 2022, nr 2(110).

Filipiak M., *Topiczna architektura platform internetowych a społeczna polaryzacja światopoglądowa*, „Journal of Modern Science" 2025, nr 3(63),

Grabkowska K., *Próba wyjaśnienia pojęcia i istoty wojen hybrydowych*, „Świat Idei i Polityki" 2022, nr 14.

Grabowska-Lepczak I., Szykuła-Piec B., Wasiluk J., *Dezinformacja jako jedno z narzędzi w wojnie hybrydowej*, „Central European Journal of Security Studies" 2024, t. 2, nr 1.

Jellinek G., *Allgemeine Staatslehre*, O. Häring, Berlin 1914.

Jurgilewicz M., *Bezpieczeństwo państwa a bezpieczeństwo jednostki*, „Modern Management Review" 2018, t. 23, nr 25(1).

Kacała T., *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2(24).

Kaźmierczak D., Laskowski M., *Social cohesion in hybrid conflicts. Case of migration crisis at the polish-belarussian border and migration flows from Ukraine*, „Przegląd Wschodnioeuropejski" 2024, nr 15.2.

Kołodziejczak M., *Analiza pojęcia wojny, agresji i napaści zbrojnej oraz przykłady ich użycia w aktach prawnych obowiązujących w Rzeczypospolitej Polskiej*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2015, nr 2(14).

Kossecki J., *Proces produkcji informacji i jego wpływ na aktywność społeczną,* „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1973, nr 4.

Kożdoń-Dębecka M., *Polaryzacja medialna na przykładzie kryzysu migracyjnego na granicy polsko-białoruskiej latem 2021 roku w relacjach trzech polskich telewizyjnych serwisów informacyjnych*, „Media Biznes Kultura" 2023, nr 1(14).

Kurczewska J., *Granica niejedno ma imię. Trzy podejścia teoretyczne* [w:] *Granice na pograniczach*, red. J. Kurczewska, H. Bojar, Wydawnictwo IFiS PAN, Warszawa 2005.

Kwiecińska M., *Nowy wymiar konfliktów zbrojnych: konflikt hybrydowy a konflikt pełzający*, „Doctrina Studia Społeczno-Polityczne" 2016, nr 13.

Likhovitskyy Y., Polián P., Svyrydiuk N., *Information Threats in the Context of Hybrid War*, „Advances in Economics, Business and Management Research 2021, nr 188.

Lubiewski P., *Granice Rzeczypospolitej Polskiej jako wyzwanie dla bezpieczeństwa państwa*, „Przegląd Policyjny" 2019, nr 0 (specjalny).

Ochmann P., *Prawne implikacje wybranych elementów terminu „wojna hybrydowa"*, „Studia Prawa Publicznego" 2019, nr 4(28).

Palczewski M., *Selekcja informacji w mediach – zasady, wartości, manipulacje*, „Naukowy Przegląd Dziennikarski" 2015, nr 2.

Pettersson J., *What's in a Line? Making Sovereignty through Border Policy*, PhD Thesis, Acta Universitatis Upsaliensis 2018.

Piejak A., *Pomiędzy wojną i pokojem – przestrzeń budowania kultury pokoju* [w:] *Humanistyczne ambiwalencje globalizacji. Zbiór studiów*, red. A. Piejak, I. Wojnar, Warszawa 2021.

Pomykała M., *Bezpieczeństwo wewnętrzne państwa wobec współczesnych zagrożeń*, „Bezpieczeństwo. Teoria i Praktyka" 2009, nr 1-2.

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 4.

Skwarski A., Szkudlarek P., *Rola informacji i zagrożenia dezinformacją w systemie bezpieczeństwa państwa*, „Studia Administracji i Bezpieczeństwa" 2020, nr 5.

Słownik terminów z zakresu bezpieczeństwa narodowego, red. J. Kaczmarek, W. Łepkowski, B. Zdrodowski, AON, Warszawa 2008.

Stankiewicz K., *Wpływ Internetu na percepcje wiarygodności informacji* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?,* red. L. Haber, t. II, Kraków 2004.

Szczygielska A., *Konflikt hybrydowy – analiza porównawcza źródeł wiedzy o zjawisku*, „Roczniki Nauk Społecznych" 2023, t. 15(51), nr 2.

Tomal D., *Wiarygodność jako argument legitymizacyjny lokalnych przywódców politycznych*, rozprawa doktorska UKEN, Kraków 2025.

Więckowski M., *Od barier i izolacji do sieci i przestrzeni transgranicznej – konceptualizacja cyklu funkcjonowania granic państwowych*, „Przegląd Geograficzny" 2019, nr 91.4.

Prawodawstwo

Konwencja z Montevideo z dnia 26 grudnia 1933 r. (UNTS nr 165).

Patrycja KAWKA[1]
Seweryn WALAS[2]

CYBERZAGROŻENIA JAKO NOWY WYMIAR KONFLIKTÓW WE WSPÓŁCZESNYCH PRZEDSIĘBIORSTWACH

Celem pracy była analiza i ocena skali oddziaływania cyberataków jako zagrożeń we współczesnych firmach. Zidentyfikowano zarówno zagrożenia zewnętrzne, takie jak złośliwe oprogramowanie, phishing, ataki DDoS, ransomware czy kradzież tożsamości, jak i zagrożenia wewnętrzne wynikające z błędów pracowników, braku świadomości bezpieczeństwa bądź działań intencjonalnych. Szczególną uwagę zwrócono na fakt, że czynnik ludzki pozostaje jednym z najsłabszych ogniw systemu cyberbezpieczeństwa, a działania socjotechniczne są często skuteczniejsze niż zaawansowane ataki techniczne. Istotnym ustaleniem jest również wskazanie czynników napędzających rozwój cyberzagrożeń, wśród których kluczową rolę odgrywają cyfryzacja usług, globalizacja procesów organizacyjnych, rozproszenie systemów informatycznych oraz dynamiczny rozwój Internetu Rzeczy. Czynniki te zwiększają powierzchnię ataku i utrudniają skuteczne zarządzanie bezpieczeństwem, zwłaszcza w przedsiębiorstwach o złożonej strukturze i transgranicznym charakterze działalności.

Słowa kluczowe: cyberbezpieczeństwo, konflikty, bezpieczeństwo cyfrowe, społeczeństwo informacyjne, bezpieczeństwo.

Wprowadzenie

Cyberprzestrzeń najprościej można ująć jako całokształt powiązań wirtualnych. W literaturze przedmiotu funkcjonuje wiele definicji. Cyberprzestrzeń określana jest także jako płaszczyzna zarówno przetwarzania, jak i wymiany informacji, która jest tworzona przez systemy teleinformatyczne. Co więcej, wzrost znaczenia cyberprzestrzeni współcześnie zarówno dla państwa, społeczeństwa oraz organizacji stwarza jeszcze większą potrzebę ochrony jej bezpieczeństwa[3]. Obecnie cyberprzestrzeń jest podstawowym obszarem działania współczesnych organizacji. Nastąpiło to wraz z szybkim rozwojem technologii w zakresie informacyjno-komunikacyjnym. Systemy informacyjne wspomagają praktycznie wszystkie procesy zachodzące w organizacjach zarówno w kontekście biznesowym jak

[1] Patrycja Kawka, studentka Politechniki Rzeszowskiej im. Ignacego Łukasiewicza, Koło Naukowe Polityki Bezpieczeństwa Państwa.
[2] Seweryn Walas, student Politechniki Rzeszowskiej im. Ignacego Łukasiewicza, Koło Naukowe Polityki Bezpieczeństwa Państwa, ORCID: 0009-0009-2488-0333.
[3] T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego,* „Przegląd Bezpieczeństwa Wewnętrznego" 2016, t. 8, nr 15, s. 11-12.

również administracyjnym. Jest to niewątpliwe udogodnienie współczesnych czasów, jednak z drugiej strony ryzyko wystąpienia różnego rodzaju cyberzagrożeń w organizacjach staje się coraz bardziej prawdopodobne. Cyberzagrożenie opisywane jest jako zjawisko bądź też działanie w cyberprzestrzeni, które w rezultacie doprowadza do naruszenia poufności systemów informatycznych organizacji oraz zawartych w nich danych. Cyberzagrożenia nie stanowią dziś jedynie problemu technicznego, lecz są postrzegane z perspektywy konfliktów, zarówno w głębi organizacji, jak również między instytucjami publicznymi oraz podmiotami gospodarczymi[4].

Aktualnie pojęcie cyberzagrożeń obejmuje zarówno typowe ataki na infrastrukturę teleinformatyczną, tj. phishing lub złośliwe oprogramowanie, jak również działania zorganizowane zachodzące w postaci cyberprzestępczości najczęściej o podłożu ekonomicznym[5]. Konsekwencje tych działań doprowadzają najczęściej do strat finansowych ponoszonych przez organizacje, jak również zakłóceń w procesach organizacyjnych, utraty zaufania klientów, co ostatecznie obniża stabilność funkcjonowania organizacji[6]. Niewątpliwie warto przyjrzeć się dokładniej pojęciu cyberprzestępczości. Wskazać należy również na brak formalnej definicji „cyberprzestępczości" w polskim prawodawstwie. Nie stanowi to jednak problemu, ponieważ obecnie dostępnych jest wiele definicji cyberprzestępczości, które stają się adekwatną podstawą do rozważania tego zagadnienia. Zgodnie z nimi najprościej cyberprzestępczość można ująć jako działania wbrew prawu, do których realizacji potrzebne są komputery, jak i urządzenia mobilne oraz sieci informatyczne i elektroniczne[7]. Zgodnie z założeniami Polityki Ochrony Cyberprzestrzeni RP cyberprzestępstwo sprowadzane jest do czynu zabronionego, którego popełnienie następuje w zasięgu cyberprzestrzeni[8]. Analizując wskazaną treść pod kątem prawnym, cyberprzestępczość dotyczy dość dużego zakresu czynów zabronionych. Wśród nich znajdują się klasyczne przestępstwa, których popełnienie zachodzi na płaszczyźnie teleinformatycznej, a idealnym przykładem w tym kontekście będą oszustwa w sferze bankowości elektronicznej. Zwrócić uwagę należy również na drugą stronę zagadnienia i jasno zaznaczyć, iż cyberprzestępstwa w znacznym stopniu bazują na wykorzystaniu informacji już istniejących poprzez działania takie jak sabotaż komputerowy.

---

[4] R. Althar, D. Samanta, M. Kaur, A. Alnuaim, N. Aljaffan, M. Ullah, *Software Systems Security Vulnerabilities Management by Exploring the Capabilities of Language Models Using NLP, "*Computational Intelligence and Neuroscience" 2021, 1, s. 1-16.

[5] G. Pilarski, *Przegląd współczesnych zagrożeń w cyberprzestrzeni*, „Wojskowy Instytut Techniczny Uzbrojenia. Problemy Techniki Uzbrojenia" 2023/52/167, s. 97-106.

[6] D. Szafranek, *Wpływ rozwoju cyberprzestępczości na funkcjonowanie współczesnych organizacji*, „Nowoczesne Systemy Zarządzania" 2021, z. 16, s. 45-47.

[7] N. Urbańska, *Cyberprzestępczość i wynikające z niej zagrożenia,* Akademia Marynarki Wojennej, Gdynia, 2025*,* s. 2.

[8] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013, s. 5.

Obecnie mamy do czynienia z dużą różnorodnością cyberprzestępczości, która powstaje na wskutek prawnych regulacji międzynarodowych, analizy zjawiska oraz wielu statystyk policyjnych obejmujących wskazany zakres. Zatem należy dokonać rozróżnienia cyberprzestępczości. W tym kontekście funkcjonują następujące rodzaje: przestępczość komputerowa, która obejmuje np. podsłuch komputerowy czy też sabotaż. Kolejnym jest przestępczość telekomunikacyjna obejmująca np. duplikowanie numeru telefonu IMEI. Natomiast ostatni rodzaj to przestępczość internetowa, której adekwatnym przykładem jest dość częste wykorzystanie nieautoryzowanego dostępu do poczty internetowej[9].

Warto przeanalizować także definicje cyberprzestępczości powstałe z inicjatywy organizacji międzynarodowych, tj. Unia Europejska, Interpol czy Organizacja Narodów Zjednoczonych. Zgodnie z zapisami na temat cyberprzestępczości stworzonymi przez Interpol, wskazane pojęcie należy rozumieć jako przestępstwa, do których dochodzi jedynie w Internecie, przy tym uwzględniając wyłączne wykorzystanie technologii elektronicznych[10]. Przechodząc do definicji Organizacji Narodów Zjednoczonych w sprawie cyberprzestępczości, wyszczególniono dwa podłoża jej analizy, a zatem w wąskim ujęciu odnosi się do czynności skierowanych przeciwko bezpieczeństwu danych lub systemów komputerowych. Natomiast jeśli chodzi o szerokie ujęcie zagadnienia, cyberprzestępczość dotyczy wszystkich nielegalnych działań dokonywanych przy użyciu sieci lub systemów komputerowych, np. nieuprawniony dostęp oraz rozprowadzanie informacji[11].

Obecnie cyberprzestępczość rozwija się błyskawicznie wraz z rozwojem technologicznym oraz mocno wyrasta poza ramy tradycyjnie pojmowanej przestępczości. Jest to bez wątpienia problem urastający do rangi zagrożenia wobec bezpieczeństwa, które charakteryzuje się swoistymi cechami. Zatem są nimi przestrzeń wirtualna, w której dochodzi do cyberprzestępstw. W tym kontekście istotna staje się trudność w przygotowaniu regulacji prawnych na poziomie krajowym, które podniosłyby poziom bezpieczeństwa, mając ciągle na uwadze ponadnarodowy charakter zjawiska. Ponadto sprawcy cyberprzestępstw najczęściej realizują swoje zadania zdalnie oraz anonimowo, co umożliwia obecnie Internet, jednak stwarza tym samym trudności w ściganiu ich sprawców. Jednym z ważniejszych aspektów związanych z cyberprzestępczością jest fakt iż ona sama nie zagraża wyłącznie jednostką jako pojedynczym obywatelom ale jest sporym zagrożeniem wobec bezpieczeństwa przedsiębiorstw, co przekłada się w dalszej części również na bezpieczeństwo państwa poprzez możliwość negatywnego wpływu na sektor finansowy, dane o znaczeniu strategicznym z punktu widzenia państwa czy też infrastrukturę krytyczną[12].

---

[9] N. Urbańska, *Cyberprzestępczość...,* dz. cyt., s. 2-4.
[10] M. Zbrojewska, *Jak definiujemy cyberprzestępstwo?*, „IAPGOŚ" 2016, 2.
[11] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem,* Wolters Kluwer Polska, Warszawa 2010, s. 55.
[12] N. Urbańska, *Cyberprzestępczość...,* dz. cyt., s. 5-6.

Obrany temat jest wart przeanalizowania z uwagi na wzrost incydentów cybernetycznych oraz ich wpływu na powstawanie sytuacji konfliktowych w organizacjach. Celem niniejszej pracy jest analiza zagrożeń, skutków i metod zapobiegania cyberzagrożeniom oraz ich roli w funkcjonowaniu współczesnych organizacji, która urasta do miana konfliktów. Cyberbezpieczeństwo w firmach jest kluczowym czynnikiem gwarantującym ich stabilne funkcjonowanie. Odgrywa istotną rolę poprzez ochronę danych, systemów informacyjnych czy też zapewnienie ciągłości w działaniu. Istotą cyberbezpieczeństwa jest identyfikacja oraz analiza zagrożeń oraz odpowiednie reagowanie w procesie ich zwalczania. Skuteczne monitorowanie zagrożeń zwiększa szanse na ich szybkie wykrywanie oraz zmniejszenie skutków ich ewentualnego wystąpienia dla organizacji[13].

Charakterystyka współczesnych cyberzagrożeń

Postęp technologiczny znacznie wpływa na funkcjonowanie człowieka, wykraczając poza sfery kultury, relacji społecznych czy edukacji i obejmuje także działalność współczesnych organizacji. Kształtowanie społeczeństwa informacyjnego stwarza nowe wyzwania, które w zależności od swojego charakteru mogą być postrzegane jako ryzyko dla współczesnych organizacji bądź inspiracja do rozwoju. Istotne w tym aspekcie jest podnoszenie świadomości odnośnie cyberzagrożeń powszechnie występujących oraz w odpowiedzi na podejmowanie odpowiednich działań zaradczych. Znajomość współczesnych cyberzagrożeń w znacznym stopniu przyczynia się do zmniejszenia podatności na takie zagrożenia oraz podnosi poziom bezpieczeństwa we współczesnych organizacjach[14].

Obecnie działając w cyberprzestrzeni zagraża nam wiele niebezpieczeństw, które zostały usystematyzowane w literaturze przedmiotu oraz dokładnie opisane. Jednym z popularniejszych cyberzagrożeń jest złośliwe oprogramowanie (malware). Jest to forma cyberataku wykorzystująca aplikacje zaprojektowane, aby skutecznie naruszać bezpieczeństwo systemów informatycznych. Do tego rodzaju oprogramowania zaliczane są wirusy komputerowe, programy umożliwiające śledzenie użytkowników czy tzw. robaki sieciowe. Działania wykorzystujące złośliwe oprogramowania są przed wszystkim nastawione na zdobycie danych poufnych, prowadzenie działań szpiegowskich, kradzież tożsamości, jak również wywołanie zakłóceń funkcjonowania usług oraz systemów informatycznych[15].

Rozpatrując zagadnienie z perspektywy prawnej powyżej opisane działanie może być kwalifikowane na podstawie art. 267 § 1 kodeksu karnego (k.k.), który penalizuje uzyskanie dostępu do informacji bez uprawnienia. Przewidziana w ustawie kara to grzywna, ograniczenie lub pozbawienie wolności do lat 2. Zastosowanie w tym przypadku znajduje także art. 268a k.k., który odnosi się do zakłócenia

[13] T. Dębowski, *Cyberbezpieczeństwo wyzwaniem XXI wieku,* Wydawnictwo Naukowe Archae-Graph, Łódź–Wrocław 2018, s. 31-34.
[14] D. Szafranek, *Wpływ rozwoju cyberprzestępczości…,* dz. cyt., s. 45-47.
[15] G. Pilarski, *Przegląd współczesnych zagrożeń…,* dz. cyt., s. 98.

pracy systemu informatycznego, kara przewidziana za popełnienie tego czynu to pozbawienie wolności do lat 3. Znamiona przestępstwa obejmują zwłaszcza działanie bez uprawnienia, a także ingerencje w dane lub system w zamiarze popełnienia czynu bezpośrednim lub ewentualnym[16].

Kolejnym istotnym zagrożeniem są ataki dokonywane poprzez strony internetowe i są one często stosowane w działaniach cyberprzestępczych. W tym rodzaju ataku sprawcy używają zarówno systemów, jak i usług dostępnych w sieci jako wektor ataku. Głównym celem jest wprowadzenie użytkownika w błąd np. poprzez fałszywe strony internetowe lub poprzez nieświadome pobranie z Internetu zainfekowanych już plików. Podstawowy cel ataku to przede wszystkim pozyskanie danych wrażliwych oraz informacji istotnych z perspektywy sprawcy ataku oraz korzyści o podłożu finansowym[17]. Tego rodzaju działania mogą wypełniać znamiona oszustwa określonego w art. 286 § 1 k.k. Istotą tego przestępstwa jest co do zasady doprowadzenie danej osoby do niekorzystnego rozporządzenia mieniem poprzez wprowadzenie jej w błąd. Przewidziana w kodeksie karnym kara za tego typu czyn to pozbawienie wolności do 8 lat. Natomiast jeśli chodzi samą ingerencję w proces przetwarzania danych, to zastosowanie ma wówczas art. 287 k.k., który przewiduje za popełniony czyn do 5 lat pozbawienia wolności[18].

Kontynuując charakterystykę cyberzagrożeń należy uwzględnić phishing. Wskazana forma ataku przejawia się poprzez podszywanie pod użytkowników w sieci. Za podstawowy cel jego przeprowadzania uchodzi zdobycie danych zwłaszcza informacji służących do uwierzytelnienia, danych finansowych lub też środków pieniężnych. Realizacja tej formy cyberataku odbywa się za pomocą wiadomości elektronicznych, które swoją treścią przypominają komunikaty od wiarygodnych osób oraz instytucji. Sprawcy ataku zależy, aby przekonać adresata potencjalnej wiadomości do skorzystania z linku prowadzącego do fałszywej strony lub uruchomienie zawirusowanego załącznika, co jest istotą ataku[19]. W kontekście prawnym phishing jest kwalifikowany jako oszustwo przewidziane w art. 286 § 1 k.k. lub oszustwo komputerowe z art. 287 k.k. Znamiona czynu obejmują działanie w celu osiągnięcia korzyści majątkowej jak również wprowadzenie w błąd oraz doprowadzenie osoby do określonego działania jakim może być ujawnienie danych[20].

Spam to dość popularna forma zagrożenia spotykana w sieci. Polega na rozprzestrzenianiu na dużą skalę niechcianych przez ich adresatów wiadomości. Takie komunikaty najczęściej są stosowane jako narzędzie aranżujące inne formy ataków, do których należy zaliczyć działania polegające na pozyskaniu danych osobowych czy też danych finansowych. Dostęp użytkownika do spamu

[16] Art. 267-268a ustawy z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn. Dz.U. z 2025 r. poz. 1872).
[17] G. Pilarski, *Przegląd współczesnych zagrożeń...,* dz. cyt., s. 98.
[18] Art. 286-287 ustawy z dnia 6 czerwca 1997 r. Kodeks karny.
[19] T. Dębowski, *Cyberbezpieczeństwo…,* dz. cyt., s. 31-34.
[20] Art. 286-287 ustawy z dnia 6 czerwca 1997 r. Kodeks karny.

w konsekwencji może doprowadzić do nieautoryzowanych działań jak np. zdobycie informacji poufnych lub instalacja złośliwego oprogramowania. Dodatkowo warto zaznaczyć, iż spam nie zawsze stanowi czyn zabroniony, jednak może pełnić funkcję narzędzia przydatnego do realizacji innych przestępstw. Z tego punktu widzenia ocena prawna czynu zależy zarówno od kontekstu oraz skutków działania sprawcy. Istotne jest również aby doszło w tym wypadku do spełnienia znamion konkretnych czynów zabronionych[21].

Atak typu DoS (ang. *Denial of Service*) skupia swoje działanie na zakłóceniu dostępności systemu komputerowego, co jest wynikiem wytwarzania zbyt dużej ilości informacji, które zdecydowanie przekraczają możliwości przetwarzania komputera. Konsekwencją tego ataku jest ograniczenie bądź całkowita utrata możliwości korzystania z systemu komputerowego. Ataki DDoS (ang. *Distrbuted Denial of Service*) są rodzajem ataku DoS, które są bardziej rozproszone oraz równocześnie wykorzystują wiele przejętych urządzeń, aby przeciążyć infrastrukturę, która jest celem ataku[22]. Powyżej opisane zachowanie podlega kwalifikacji prawnej na podstawie art. 268a k.k., który to artykuł penalizuje istotne zakłócenia pracy systemu informatycznego. Do znamion czynu zalicza się działanie polegające na ingerencji w funkcjonowanie systemu, a także wywołanie skutku w postaci ograniczenia dostępności do takiego systemu[23].

Powszechnie znane zagrożenie, które dotyka swoimi konsekwencjami obecnie wiele osób to kradzież tożsamości. Ta forma polega na wykorzystaniu danych osobowych, aby podszyć się pod inną osobę oraz zdobyć założone korzyści najczęściej finansowe. Dane, które podlegają kradzieży, to przede wszystkim szeroko pojęte dane osobowe w tym adres zamieszkania oprócz tego dane oraz numery kart oraz kont bankowych, hasła dostępu oraz adresy do poczty elektronicznej. Kradzież danych niesie za sobą konsekwencje zarówno dla poszkodowanych, których dane zostały skradzione jak również dla organizacji, które odpowiadają za ich przetwarzanie oraz bezpieczeństwo[24]. Opisane zachowanie w kodeksie karnym zostało ujęte w art. 190a § 2. Znamiona tego czynu obejmują podszywanie się pod inną osobę oraz wykorzystanie jej danych osobowych lub wizerunku do celów wyrządzenia szkody zarówno majątkowej, jak i osobistej. Za wskazany czyn przewidziana została kara pozbawienia wolności do 8 lat[25].

Wśród zagrożeń warto przedstawić zagrożenia wewnętrzne, a zatem te, które są powodowane przez osoby związane z daną organizacją lub jej współpracownikami, których działania mogą być powodem naruszenia bezpieczeństwa. Specyfika tych zagrożeń jest złożona, mogą one wynikać zarówno z braku dostatecznej

---

[21] G. Pilarski, *Przegląd współczesnych zagrożeń…,* dz. cyt., s. 99.

[22] A. Połowin, *Cyberzagrożenia w internecie – analiza przypadków,* „Cybersecurity and Law" 2024, nr 2(12), s. 118-125.

[23] Art. 268a ustawy z dnia 6 czerwca 1997 r. Kodeks karny.

[24] M. Kliś, *Przestępczość w internecie. Zagadnienia podstawowe,* „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1, s. 99.

[25] Art. 190a ustawy z dnia 6 czerwca 1997 r. kodeks karny.

wiedzy przez pracownika lub też z celowego działania na niekorzyść organizacji. Wskazana postać zagrożenia jest istotna ze względu na fakt, że sprawcy to osoby działające wewnątrz danej struktury, co czyni takie zagrożenie trudniejszym do wykrycia. W zależności od charakteru popełnionego czynu mogą one wypełniać znamiona różnych przestępstw, w tym będzie to naruszenie poufności informacji lub też zakłócenie funkcjonowania systemu[26].

Bardzo niebezpieczne są dla wielu organizacji zagrożenia związane z wyciekiem informacji. O tym zagrożeniu można mówić wówczas, gdy dane poufne trafią do osób oraz podmiotów nieuprawnionych, które nie powinny ich przetwarzać. Konsekwencją wycieku informacji dla organizacji są najczęściej zarówno straty finansowe, jak również utrata zaufania ze strony klientów oraz reputacji na rynku, jednak kluczowa jest utrata prywatności. Do wycieków informacji najczęściej dochodzi poprzez ataki socjotechniczne lub też korzystanie z niezabezpieczonych sieci[27] W zależności od okoliczności zaistnienia zdarzenia mogą one skutkować zarówno odpowiedzialnością karną z art. 267 k.k. lub też odpowiedzialnością administracyjną na postawie przepisów ustawy o ochronie danych osobowych. Najważniejsze znamiona obejmują bezprawne ujawnienie danych oraz naruszenie obowiązku ich ochrony[28].

Oprogramowanie typu ransomware obecnie jest popularniejszym środkiem stosowanym przez cyberprzestępców. Algorytm działania polega na blokowaniu dostępu do systemów lub też danych ofiary, po czym wymagany jest okup za ich przywrócenie. Niewątpliwie rozwój technologii oraz sieci komputerowych stwarza szansę, ale również generuje poważne zagrożenia. Ransomware jest jednym z głównych zagrożeń w cyberprzestrzeni, które w konsekwencji prowadzi do sporych obciążeń finansowych dla zaatakowanych użytkowników oraz organizacji[29]. W zależności od sposobu działania sprawcy czyn ten może być kwalifikowany jako oszustwo z art. 286 k.k. zakłócenie działania systemu informatycznego z art. 268a k.k. lub też jako wymuszenie rozbójnicze z art. 282 k.k., za które przewidziana jest kara pozbawienia wolności do 10 lat. Znamiona w szczególności odnoszą się do osiągnięcia korzyści majątkowej oraz wpłynięcia do ofiarę poprzez wywarcie bezprawnej presji[30].

Czynniki warunkujące cyberzagrożenia

Po dokonaniu charakterystyki najistotniejszych zagrożeń występujących w cyberprzestrzeni warto rozpatrzyć czynniki, które napędzają proces ich rozwoju. Wśród nich należy wskazać cyfryzację usług oraz procesów. Obecnie znaczna część usług oraz procesów jest przenoszona do środowiska elektronicznego.

[26] M. Kliś, *Przestępczość w internecie...*, dz. cyt., s. 101-105.
[27] G. Pilarski, *Przegląd współczesnych zagrożeń…,* dz. cyt., s. 100.
[28] T. Dębowski, *Cyberbezpieczeństwo...*, dz. cyt., s. 35-38.
[29] A. Połowin, *Cyberzagrożenia w internecie...,* dz. cyt., s. 125-129.
[30] Art. 282 ustawy z dnia 6 czerwca 1997 r. Kodeks karny.

Chociaż płyną z tego zauważalne korzyści fakt powszechnej cyfryzacji, buduje ryzyko oraz zwiększa podatność na cyberataki. Do środowiska cyfrowego przenoszone są kluczowe obszary działalności zarówno administracyjnych, komunikacyjnych, jak i operacyjnych. Cyfryzacja w znacznym stopniu pozytywnie wpływa na osiągalność usług oraz ich wydajność, jednak wraz z tym rośnie ryzyko wystąpienia działań cyberprzestępczych. Zwiększająca się zależność organizacji od cyfrowych technologii generuje ryzyko zarówno w postaci strat finansowych organizacji jej renomy oraz zakłóceń w jej funkcjonowaniu. Wśród kluczowych usług, w których cyfryzacja pełni zasadniczą rolę, znajdują się: transport, ochrona zdrowia, finanse oraz energetyka. Równocześnie te sektory są w sposób szczególny narażone na cyberataki oraz konsekwencje z nimi związane[31].

Zasadniczy wpływ na rozwój cyberzagrożeń mają również globalizacja oraz rozwój rozproszonych systemów informatycznych. Obecnie, organizacje działają w oparciu o struktury międzynarodowe, globalne łańcuchy dostaw i chmurę obliczeniową. Wszystko to prowadzi do zwiększenia liczby powiązań między systemami informacyjnymi, co z kolei wpływa na powstawanie podatności na wystąpienie cyberataku. Warto zaznaczyć, że rozproszenie systemów informatycznych utrudnia efektywne zarządzanie bezpieczeństwem. Wynika to z konieczności uwzględnienia różnych sposobów ochrony, rozwoju technologicznego oraz regulacji prawnych, które występują w poszczególnych krajach. Ataki cybernetyczne mogą być przeprowadzone na dużą skalę na podstawie pojedynczej podatności, która występuje u jednego z partnerów biznesowych lub dostawców technologii. W ten sposób globalizacja i rozproszenie systemów są jednym z czynników wpływu na intensywność cyberzagrożeń, a także na podejście do bezpieczeństwa cyberprzestrzeni.

Czynnikiem wpływu na rozwój cyberzagrożeń jest także Internet Rzeczy, który obejmuje rozległą sieć urządzeń, których połączenie ma na celu wymianę danych oraz automatyzację procesów w sektorze przemysłowym, jak również w gospodarstwach domowych. Rozproszenie urządzeń oraz panująca obecnie różnorodność technologiczna nie wpływają korzystnie na zarządzanie bezpieczeństwem, a zwłaszcza w tym kontekście zachodzi większe prawdopodobieństwo wystąpienia działań cybernetycznych. Dosłownie każde urządzenie podłączone do sieci, a zatem urządzenia mobilne czy też inteligentne systemy przemysłowe potencjalnie stają się punktem rozpoczynającym ataki cybernetyczne. Wraz ze wzrostem liczby urządzeń podłączonych do sieci ryzyko ataku cybernetycznego jest znacznie większe[32].

Obecne środowisko cyberbezpieczeństwa narażone jest na różnorodne zagrożenia, a ich skuteczność zależy od wykorzystania przez sprawców różnych

[31] Parlament Europejski, *Dlaczego cyberbezpieczeństwo jest ważne i jakie są koszty cyberataków?* https://www.europarl.europa.eu/topics/pl/article/20211008STO14521/dlaczego-cyberbezpieczenstwo-jest-wazne-i-jakie-sa-koszty-cyberatakow (dostęp: 15.01.2026 r.).

[32] Ch. Biedermann, *Cybersecurity and the Internet of Things*, "Zagadnienia Informacji Naukowej" 2016, t. 2, nr 108, s. 22-36.

wektorów ataku. Funkcjonuje podział na dwa rodzaje wektorów ataku, do których zaliczone są techniczne wektory oraz te związane z działalnością człowieka, czyli poprzez błędy ludzkie[33].

Techniczne wektory ataku są związane z infrastrukturą techniczną, która w tym przypadku stanowi kluczowy punkt przeprowadzenia cyberataku. To właśnie oprogramowania, sieci oraz urządzenia stają się drogą, która ułatwia cyberprzestępcom wejście do systemu oraz skuteczny atak[34].

Jedną z najważniejszych płaszczyzn ataku jest sieć, która umożliwia komunikację zarówno pomiędzy systemami jak również użytkownikami. Wśród ataków sieciowych pojawiają się formy takie jak ataki DDoS lub sniffing, czyli podsłuchiwania ruchu. Działania te opierają się w znacznym stopniu na zakłócaniu lub modyfikacji transmisji danych lub jej przechwytywaniu. Często skutecznie przeprowadzony atak sieciowy jest dowodem na brak wystarczających zabezpieczeń systemu lub brak nie zaktualizowanych urządzeń sieciowych. Znaczna większość incydentów sieciowych jest konsekwencją braku implementacji mechanizmów bezpieczeństwa oraz pojawiające się błędy w konfiguracji[35].

Inną metodą ataku są aplikacje webowe oraz strony internetowe. Z uwagi, że są one dostępne powszechnie, są szczególnie narażone na atak. W znacznym stopniu podatności na zagrożenie atakiem są spowodowane niewłaściwą weryfikacją danych wejściowych lub błędami dotyczących kodu. Na możliwość wystąpienia ataku znacząco wpływają zarówno błędy programistyczne oraz niewystarczające sprawdzenie danych wejściowych, które tworzą lukę w oprogramowaniu, a ta z kolei może być wykorzystana do próby atak[36].

Urządzenia mobilne wyposażone w system Android lub iOS oraz wszelkie inne związane z nimi aplikacje obecnie są częstym celem ataków zwłaszcza w kontekście dynamicznego rozwoju Internetu Rzeczy w organizacjach. Wśród zagrożeń związanych z urządzeniami mobilnymi najczęściej pojawiają się ataki phishingowe przeprowadzane za pomocą wiadomości push lub tradycyjnych SMS. Do ataku wykorzystywane są także luki w systemach operacyjnych, które pojawiają się w wyniku opóźnionych aktualizacji oprogramowania czy też słabego zarządzania uprawnieniami w aplikacjach[37].

Kluczowym sposobem ataku są także luki w oprogramowaniu oraz słaba konfiguracja systemów. Luka w oprogramowaniu może zostać wykorzystana w celu uzyskania dostępu do zasobów chronionych, wygenerowania nieautoryzowanego kodu lub rozszerzenia uprawnień. Dodatkowo, spora część incydentów cyberne-

[33] W. Stallings, *Network Security Essentials Applications and Standards*, Pearson, England 2017, s. 17-42.
[34] Tamże, s. 17-42.
[35] Tamże, s. 21-40.
[36] H. Shahriar, *An Exploratory Analysis of Mobile Security Tools,* Kennesaw State University, 2019, s. 1-16.
[37] Tamże, s. 1-13.

tycznych jest związana z zaniedbaniami w kwestii przeprowadzania aktualizacji oraz konfiguracji[38].

Pomiędzy technologicznymi aspektami bezpieczeństwa w cyberprzestrzeni bardzo ważną rolę odgrywa również człowiek. W znacznym stopniu na bezpieczeństwo wpływają zachowania oraz błędy pracowników organizacji, w tym także ich skłonność do ulegania manipulacji. Powszechnie wykorzystywanym wektorem do przeprowadzenia ataków w tej kategorii są błędy użytkowników. Wśród nich znajdują się m.in.: stosowanie słabych haseł prostych w złamaniu, stosowanie równocześnie tych samych haseł w kilku systemach. Błędy ludzkie często prowadzą do ujawnienia danych uwierzytelniających lub też do wprowadzenia złośliwego kodu, co wynika często z otworzenia niebezpiecznego załącznika. Odpowiednie zachowanie użytkowników oraz ich ostrożność w połączeniu z systemami ochrony znacznie wpływają na poziom bezpieczeństwa, aby skutecznie chronić się przed incydentami bezpieczeństwa należy dbać o te dwa kluczowe aspekty. Niestety, jednak same systemy ochrony bez zachowania podstawowych zasad bezpieczeństwa w sieci nie zapewnią odpowiedniego poziomu cyberbezpieczeństwa[39].

Istotne w tej kategorii wektorów ataku są także socjotechniki stosowane na użytkownikach. Jest to nic innego jak manipulacja, której celem jest nakłonienie osoby do wykonania danej przez sprawcę ataku czynności lub też ujawnienia danych. Często w tym kontekście wykorzystywany jest phishing, pretexting lub też baiting. Zastosowanie socjotechniki jest o wiele prostsze od przeprowadzania ataków technicznych. Socjotechniki oparte są na manipulacji, wykorzystaniu niewiedzy oraz braku czujności użytkownika czy jego nawyków. W tym przypadku nie wymagany jest poziom wiedzy z zakresu technologicznego[40].

Skutki cyberzagrożeń dla firm

Cyberzagrożenia są współczesnym wyzwaniem dla organizacji, a dodatkowo niemożliwe jest ich całkowite wyeliminowanie. Z uwagi na powszechne działanie organizacji w cyberprzestrzeni można jedynie zapobiegać ewentualnemu wystąpieniu ataków cybernetycznych oraz zachowywać ogólne zasady bezpieczeństwa. Każdy incydent bezpieczeństwa, do jakiego dochodzi, w większym lub mniejszym stopniu generuje negatywne konsekwencje, które organizacja ponosi. W tym kontekście mogą być one natychmiastowe lub długofalowe oraz znacząco oddziaływać na funkcjonowanie organizacji oraz jej reputację[41].

---

[38] R. Althar, D. Samanta, M. Kaur, A. Alnuaim, N. Aljaffan, M. Ullah, *Software Systems Security…,* dz. cyt., s. 1-16.

[39] C. Hadnagy, *Social Engineering: The Science of Human Hacking,* Copyright Wiley 2011, s. 233-248.

[40] Tamże, s. 235-248.

[41] L. Kowalczyk, F. Mroczko, *Stan i wyzwania. Zarządzanie operacyjne w teorii i praktyce organizacji biznesowych, publicznych i pozarządowych*, Wyższa Szkoła Zarządzania i Przedsiębiorczości, Wałbrzych 2018, s. 95-102.

Wśród konsekwencji ponoszonych przez organizacje na skutek cyberataku są m.in. koszty finansowe, które występują natychmiast. Najczęściej organizacje tracą swoje zyski z działalności zarówno poprzez konieczność zawieszenia działalności, jak i poprzez utratę zaufania klientów. Dodatkowo koszty finansowe są związane z usuwaniem szkód powstałych w wyniku ataku, w tym uwzględniona jest diagnostyka, przywracanie systemów oraz zakup nowych zabezpieczeń, jak i pokrycie kosztów wynagrodzeń dla specjalistów działających w tym zakresie. Jeśli doszło do wycieku oraz naruszenia danych osobowych lub informacji poufnych, organizacje są również zobligowane do wypłacenia odszkodowań klientom lub partnerom biznesowym. Skala poniesionych kosztów jest uzależniona od stopnia zaistniałych szkód oraz wielkości danej organizacji, dlatego koszty w zależności od sytuacji mogą znacząco się różnić[42].

Cyberzagrożenia negatywnie oddziałują na ogólne funkcjonowaniu organizacji pod względem operacyjnym. Wystąpienie cyberataku generuje przerwy w działalności systemów informatycznych, a to bezpośrednio wpływa na realizację zadań i tym samym powoduje opóźnienie wykonywania usług. Dodatkowo występuje ryzyko związane z utratą danych operacyjnych, a także informacji poufnych oraz strategicznych istotnych dla organizacji. Cyberataki w dużej mierze mogą zakłócić świadczenie kluczowych usług związanych z bezpieczeństwem obywateli oraz klientów organizacji należą do nich np. usługi sektora finansowego, zdrowotnego czy też energetycznego. Warto podkreślić dotkliwość skutków dla organizacji, które w zdecydowanej większości do realizacji swoich celów oraz zadań biznesowych polegają na systemach cyfrowych[43].

Cyberzagrożenia negatywnie wpływają także na wymiar społeczny oraz reputację danej organizacji. Związane jest to zwłaszcza z utratą dotychczasowego zaufania zarówno klientów, jak i partnerów biznesowych. W dobie mediów społecznościowych trudno zatrzymać przepływ informacyjny, negatywne skutki cyberzagrożeń natychmiast stają się nagłośnione wpływając niekorzystnie na reputację organizacji oraz pozycję konkurencyjną na rynku. Takie konsekwencje wiążą się nie tylko z utratą stałych klientów, ale również mogą dotyczyć utraty dotychczasowych pracowników organizacji[44].

Cyberzagrożenia w organizacji stwarzają konsekwencje na płaszczyźnie obowiązującego prawa. Zgodnie z przepisami związanymi z ochroną danych osobowych organizacje, w których doszło do wycieku danych osobowych są zobowiązane do zgłoszenia tego typu incydentów odpowiednim organom. Dodatkowo nieprzestrzeganie przepisów prawa w tym zakresie wiąże się zarówno z karami finansowymi, jak również odpowiedzialnością administracyjną. Zadaniem organizacji jest przede wszystkim działanie na rzecz redukcji wystąpienia ryzyka naruszeń. W tym zakresie znaczenie ma przeprowadzenie audytów, przygotowanie procedur reagowania na incydenty oraz polityki bezpieczeństwa informacji. Skutki

[42] Tamże, s. 95-102.
[43] Tamże, s. 95-102.
[44] Tamże, s. 100.

cyberzagrożeń dla organizacji są wieloaspektowe oraz uderzają zarówno w wymiar finansowy, operacyjny, społeczny oraz prawny. Każdy incydent bezpieczeństwa stwarza określone konsekwencje dla organizacji, które mogą być zarówno bezpośrednie, jak i pośrednie. Dlatego więc kluczowe jest zarządzanie cyberbezpieczeństwem w sposób kompleksowy uwzględniając wszystkie aspekty skutków takich incydentów[45].

Skuteczne zapobieganie cyberzagrożeniom wymaga podejścia systemowego i wielowarstwowego, które integruje środki techniczne, organizacyjne, proceduralne i edukacyjne. Raport ENISA analizujący krajobraz zagrożeń w sektorze administracji publicznej w UE za rok 2024 wskazuje, że konieczność takiego podejścia wynika z bardzo wysokiej liczby ataków o zróżnicowanej charakterystyce, przy jednoczesnym niskim poziomie dojrzałości cyberbezpieczeństwa wielu podmiotów[46].

Firewalle są podstawową barierą ochronną w architekturze bezpieczeństwa IT, monitorując i filtrując ruch sieciowy między strefami sieci zaufanej i niezaufanej. Ich implementacja umożliwia blokowanie nieautoryzowanych połączeń, ograniczając powierzchnię ataku i minimalizując ryzyko wykorzystania podatności infrastrukturalnych. W kontekście zagrożeń takich jak np. DDoS, firewalle w połączeniu z warstwową kontrolą dostępu stanowią fundament technicznego systemu obrony.

Systemy IDS/IPS (*Intrusion Detection/Prevention Systems*) umożliwiają wykrywanie anomalii i podejrzanych zachowań w ruchu sieciowym oraz aktywne przeciwdziałanie próbom naruszenia bezpieczeństwa. IDS analizuje ruch pod kątem wzorców ataków, natomiast IPS blokuje podejrzane aktywności w czasie rzeczywistym. Raport ENISA podkreśla, że wiele ataków zarówno DDoS, jak i intruzje prowadzone przez zaawansowane grupy cyberprzestępcze można skuteczniej identyfikować i neutralizować dzięki warstwie detekcji i prewencji, co znacząco podnosi odporność systemów instytucji krytycznych.

Szyfrowanie stanowi kluczowy element ochrony informacji zarówno w spoczynku (np. na dyskach i w bazach danych), jak i w tranzycie (np. pomiędzy klientem a serwerem). Zagrożenia związane z naruszeniami danych i incydentami eksfiltracji informacji identyfikowane są jako jedne z najczęstszych i najbardziej dotkliwych szczególnie gdy dotyczą danych wrażliwych. Odpowiednio wdrożone mechanizmy kryptograficzne (np. TLS, szyfrowanie dysków, klucze asymetryczne) ograniczają skutki wycieków oraz utrudniają ich dalsze wykorzystanie, nawet w przypadku naruszenia systemów.

Podejście systemowe zakłada, że organizacja musi regularnie identyfikować, oceniać i monitorować ryzyka cybernetyczne. Zarządzanie ryzykiem to proces, który obejmuje identyfikację zagrożeń, ocenę ich potencjalnych skutków oraz priorytety działań zabezpieczających. Niska dojrzałość cyberbezpieczeństwa wielu podmiotów administracji publicznej zwiększa ich podatność na incydenty,

[45] Tamże, s. 101-102.
[46] Raport *ENISA Sectorial Threat Landscape: Public Administration*, Ateny 2025, s. 15.

dlatego konieczne są regularne audyty, które wykrywają luki konfiguracyjne, słabości procedur oraz niezgodności z dobrymi praktykami. Działania te wspierają kontekstową ocenę ryzyka i umożliwiają wdrożenie adekwatnych środków ochronnych.

Polityki bezpieczeństwa informacji stanowią formalny zestaw zasad i reguł określających ramy działania organizacji w zakresie ochrony informacji. Obejmują zarówno obowiązki pracowników, jak i technologiczne wymagania dotyczące konfiguracji, monitoringu, reagowania na incydenty czy klasyfikacji danych. W rekomendacjach dla sektora publicznego zwraca się szczególną uwagę na potrzebę spójnych, zintegrowanych polityk, które są zgodne z wymogami NIS2[47], ponieważ tylko kompleksowe wytyczne mogą zapewnić jednolity poziom bezpieczeństwa w całej organizacji i jej systemach IT.

Raport ENISA wskazuje, że wiele incydentów wykorzystywało metody socjotechniczne i ataki z użyciem phishingu[48], czyli techniki nastawione na obejście zabezpieczeń poprzez manipulację użytkownikiem. Dlatego kluczowym elementem podejścia systemowego jest budowanie kultury bezpieczeństwa oraz cykliczne szkolenia personelu. Działania te zwiększają świadomość zagrożeń, doskonalą umiejętność rozpoznawania prób oszustwa oraz ułatwiają przestrzeganie wewnętrznych procedur i polityk. Ponadto szkolenia powinny obejmować zarówno techniczne aspekty bezpieczeństwa, jak i odpowiedzialne zachowania użytkowników, co przekłada się na zdolność organizacji do adaptacji w obliczu nowych wektorów ataku.

Organizacje, które chcą skutecznie przeciwdziałać cyberzagrożeniom, muszą funkcjonować nie tylko w izolacji, lecz także jako część sieci współdziałania na poziomie krajowym i międzynarodowym. ENISA rekomenduje korzystanie z usług i wymiany informacji prowadzonych przez zespoły reagowania na incydenty (CERT/CSIRT), które oferują analizy zagrażających kampanii, wsparcie techniczne w identyfikacji i neutralizacji ataków oraz działania koordynacyjne między podmiotami dotkniętymi podobnymi incydentami. Takie partnerstwo jest szczególnie istotne w sytuacjach, gdy ataki mają charakter rozproszony, transgraniczny lub prowadzony przez zaawansowane grupy cyberprzestępcze czy państwowe.

Skuteczna prewencja, oparta na ww. elementach, znacząco redukuje ryzyko eskalacji konfliktów cybernetycznych. Dzięki kompleksowej ochronie, organizacje są w stanie wcześniej wykrywać próby naruszeń, minimalizować ich skutki oraz szybciej reagować na incydenty. Systemowe podejście do cyberbezpieczeństwa uwzględniające technologie, zarządzanie ryzykiem, polityki, edukację oraz współpracę przyczynia się do zwiększenia odporności organizacji na złożone

[47] Dyrektywa NIS2 to unijne prawne narzędzie mające na celu wzmocnienie cyberbezpieczeństwa w całej Unii Europejskiej czyli ochrony sieci i systemów informatycznych przed cyberzagrożeniami i różnymi incydentami. https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=pl (dostęp: 16.01.2026 r.).

[48] G. Pilarski, *Przegląd współczesnych zagrożeń…,* dz. cyt., s. 97-106.

i wielowektorowe ataki, które są charakterystyczne dla współczesnych środowisk konfliktów informacyjnych i cyberstrategicznych.

Cyberatak na EuroCert jako przejaw konfliktu informacyjnego

W kontekście współczesnych zagrożeń cybernetycznych przejawy konfliktów informacyjnych można najlepiej zilustrować poprzez analizę realnych incydentów. Jednym z najpoważniejszych takich zdarzeń w Polsce w pierwszym kwartale 2025 r. był atak typu ransomware[49] na firmę EuroCert Sp. z o.o. dostawcę kwalifikowanych usług zaufania, w tym podpisów elektronicznych, pieczęci kwalifikowanych oraz certyfikatów zgodnych z regulacją eIDAS (*Electronic Identification, Authentication and Trust Services*)[50], wykorzystywanych przez podmioty publiczne i prywatne do uwierzytelniania dokumentów oraz bezpiecznej komunikacji w systemach elektronicznych.

W nocy z 12 na 13 stycznia 2025 roku systemy EuroCert zostały zaatakowane przez nieznanych sprawców wykorzystujących złośliwe oprogramowanie typu ransomware, które zaszyfrowało zasoby serwerowe przedsiębiorstwa. Skróty działań operacyjnych wskazują, że atakujący uzyskali nieautoryzowany dostęp do infrastruktury IT, co doprowadziło do skompromitowania zarówno poufności, jak i dostępności danych osobowych klientów, kontrahentów oraz pracowników tej firmy. Oficjalne komunikaty EuroCert wskazują, że zaraz po wykryciu incydentu podjęto działania mające na celu ograniczenie zakresu naruszenia, m.in. zawiadomiono odpowiednie organy ścigania, CERT Polska, Policję oraz Prezesa Urzędu Ochrony Danych Osobowych (UODO), zgodnie z obowiązkiem zgłoszenia naruszenia na podstawie Rozporządzenia o Ochronie Danych Osobowych (RODO)[51].

Analiza dostępnych danych operacyjnych wskazuje, że incydent mógł doprowadzić do wycieku szerokiego zakresu danych osobowych. Mogły zostać ujawnione m.in.:

- imiona i nazwiska osób fizycznych,
- dane identyfikacyjne (PESEL, data urodzenia),
- dane kontaktowe (adresy e-mail, numery telefonów),
- szczegóły dokumentów tożsamości (seria i numer dowodu lub paszportu),
- nazwy użytkowników oraz hasła, a w niektórych przypadkach wizerunki osób wynikające z procesów weryfikacji zdalnej.

---

[49] Tamże, s. 101.

[50] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, s. 73 ze zm.).

[51] EuroCert, *Atak na EuroCert – oświadczenie*, https://eurocert.pl/atak-na-eurocert-oswiadczenie/ (dostęp: 15.01.2026 r.).

Warto podkreślić, że pomimo naruszenia danych osobowych, zgodnie z komunikatem organizacji nie doszło do kompromitacji kwalifikowanych certyfikatów cyfrowych ani kluczy kryptograficznych związanych z usługami kwalifikowanymi. Elementy te pozostały bezpieczne, a użytkownicy chmurowej usługi ECSigner zostali zobligowani do resetu haseł wraz z wykorzystaniem dwuskładnikowego uwierzytelniania.

Raporty ekspertów naniosły na obraz incydentu także potencjalny wpływ na większe ekosystemy organizacyjne w zestawieniu incydentów za luty 2025 roku wskazano, że poszkodowanymi stronami były zarówno podmioty indywidualne, jak i instytucje publiczne oraz kluczowe spółki (np. przewoźnicy, instytucje finansowe i korporacje)[52].

Analiza skutków ataku wskazuje na wielowymiarowy wpływ zdarzenia na działalność organizacji oraz jej otoczenia. W wymiarze operacyjnym incydent spowodował przerwy w funkcjonowaniu usług certyfikacyjnych, co wiązało się z ograniczeniami w autoryzacji dokumentów elektronicznych i cyfrowych procesach prowadzenia spraw w wielu instytucjach i przedsiębiorstwach. Utrata dostępności danych oraz potencjalna dostępność danych osobowych stanowiła również istotne ryzyko naruszenia praw i wolności osób, których dane zostały ujawnione, m.in. poprzez możliwość:

- wykorzystania ich danych do ataków phishingowych,
- zakładania kont podszywających się pod osoby poszkodowane,
- podejmowania prób wyłudzeń kredytowych lub pożyczek w instytucjach niebankowych.

W odpowiedzi na incydent Pełnomocnik Rządu ds. Cyberbezpieczeństwa podkreślił utrzymujące się wysokie ryzyko występowania podobnych ataków oraz konieczność przeglądu infrastruktury informatycznej oraz systemów powiązanych z usługami EuroCert, w tym blokowania zdalnych połączeń oraz szczegółowej analizy logów systemowych w celu identyfikacji luk działania te mają charakter prewencyjny oraz naprawczy.

Przypadek EuroCert uwypukla znaczenie monitorowania zagrożeń bezpieczeństwa jako elementu strategii ograniczania skutków konfliktów informacyjnych. Wczesne wykrycie incydentu oraz szybkie zawiadomienie odpowiednich służb pozwoliły na ograniczenie dalszego rozprzestrzeniania się ataku oraz identyfikację potencjalnych wektorów naruszeń. Jednocześnie przykład ten potwierdza, że samo wdrożenie zabezpieczeń technicznych nie jest wystarczające bez odpowiednio zorganizowanych procedur monitoringu, reagowania kryzysowego i współpracy z instytucjami krajowymi oraz międzynarodowymi.

[52] CyberDefense24, *Co ujawnia analiza ataku na EuroCert? Ponad 100 polskich instytucji pod lupą,* https://cyberdefence24.pl/cyberbezpieczenstwo/co-ujawnia-analiza-ataku-na-eurocert-ponad-100-polskich-instytucji-pod-lupa (dostęp: 16.01.2026 r.).

Studium ataku na EuroCert wykazuje, że:

- cyberataki klasy ransomware mają charakter konfliktowy, a więc stanowią formę presji informacyjnej i ekonomicznej, mogącej destabilizować krytyczne procesy organizacji i ich partnerów,
- poufność i dostępność danych osobowych są kluczowymi obszarami narażonymi na naruszenia, a ich kompromitacja rodzi dalekosiężne skutki społeczne oraz prawne,
- kompleksowy monitoring zagrożeń, w tym automatyczna analiza zdarzeń oraz stała współpraca z CSIRT/CERT, jest konieczny, by minimalizować skutki incydentów oraz ograniczać eskalację konfliktów cybernetycznych.

Analiza tego przypadku dostarcza cennych danych w kontekście budowy odporności organizacyjnej na cyberkonflikty oraz wskazuje praktyczne kierunki działań prewencyjnych i reaktywnych, zgodnych z zasadami monitorowania i zarządzania zagrożeniami bezpieczeństwa.

Podsumowanie

Przeprowadzona analiza potwierdza, że cyberzagrożenia stanowią obecnie jeden z kluczowych wymiarów konfliktów zachodzących we współczesnych organizacjach, zarówno w ujęciu wewnętrznym, jak i zewnętrznym. Dynamiczny rozwój technologii informacyjno-komunikacyjnych, postępująca cyfryzacja procesów oraz rosnąca zależność organizacji od systemów teleinformatycznych sprawiają, że cyberprzestrzeń stała się podstawowym obszarem ich funkcjonowania, a jednocześnie areną narastających napięć i zagrożeń o charakterze konfliktowym. Cyberzagrożenia nie ograniczają się już wyłącznie do sfery technicznej, lecz coraz częściej wpływają na relacje organizacyjne, stabilność procesów decyzyjnych, reputację podmiotów oraz zaufanie interesariuszy.

Podkreślono także wielowymiarowy charakter skutków cyberzagrożeń dla organizacji. Obejmujący nie tylko straty ekonomiczne i operacyjne, ale również konsekwencje społeczne, reputacyjne oraz prawne. Cyberataki mogą prowadzić do paraliżu działalności operacyjnej, utraty danych, naruszenia prywatności oraz odpowiedzialności regulacyjnej wynikającej z przepisów prawa, w tym RODO i dyrektywy NIS 2. Tym samym cyberzagrożenia należy postrzegać jako czynnik destabilizujący funkcjonowanie organizacji oraz potencjalne źródło długotrwałych konfliktów organizacyjnych i informacyjnych. Szczególną wartość poznawczą wnosi analiza studium przypadku cyberataku ransomware na firmę EuroCert, który unaocznia, że współczesne incydenty cybernetyczne mogą mieć charakter konfliktów informacyjnych o szerokim zasięgu oddziaływania. Przypadek ten pokazuje, że nawet organizacje pełniące kluczową rolę w ekosystemie zaufania cyfrowego są narażone na poważne naruszenia, których skutki wykraczają poza sam podmiot i dotykają jego klientów, partnerów oraz instytucje publiczne. Atak na EuroCert potwierdza, że cyberzagrożenia mogą być narzędziem presji

ekonomicznej i organizacyjnej, prowadzącym do destabilizacji procesów o znaczeniu krytycznym.

Podsumowując, cyberzagrożenia należy uznać za trwały i nieodłączny element współczesnych konfliktów w organizacjach funkcjonujących w społeczeństwie informacyjnym. Ich znaczenie będzie rosło wraz z dalszą cyfryzacją procesów i rozwojem technologii. Cyberbezpieczeństwo przestaje być wyłącznie kwestią techniczną, a staje się obszarem strategicznym, decydującym o stabilności, odporności i zdolności organizacji do funkcjonowania w warunkach narastających konfliktów informacyjnych i cybernetycznych.

Bibliografia

Aleksandrowicz T.R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego,* "Przegląd Bezpieczeństwa Wewnętrznego" 2016, t. 8, nr 15.

Althar R., Samanta D., Kaur M., Alnuaim A., Aljaffan N., Ullah M., *Software Systems Security Vulnerabilities Management by Exploring the Capabilities of Language Models Using NLP, "*Computational Intelligence and Neuroscience" 2021, 1.

Biedermann Ch., *Cybersecurity and the Internet of Things*, "Zagadnienia Informacji Naukowej" 2016, t. 2, nr 108.

Dębowski T., *Cyberbezpieczeństwo wyzwaniem XXI wieku,* Wydawnictwo Naukowe ArchaeGraph, Łódź–Wrocław 2018.

Hadnagy C., *Social Engineering: The Science of Human Hacking,* Copyright Wiley 2011.

Kliś M., *Przestępczość w internecie. Zagadnienia podstawowe,* „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.

Kowalczyk L., Mroczko F., *Stan i wyzwania. Zarządzanie operacyjne w teorii i praktyce organizacji biznesowych, publicznych i pozarządowych*, Wyższa Szkoła Zarządzania i Przedsiębiorczości, Wałbrzych 2018.

Pilarski G., *Przegląd współczesnych zagrożeń w cyberprzestrzeni*, „Wojskowy Instytut Techniczny Uzbrojenia. Problemy Techniki Uzbrojenia" 2023/52/167.

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013.

Połowin A., *Cyberzagrożenia w internecie – analiza przypadków,* „Cybersecurity and Law" 2024, nr 2(12).

Raport ENISA Sectorial Threat Landscape: Public Administration, Ateny 2025.

Shahriar H., *An Exploratory Analysis of Mobile Security Tools,* Kennesaw State University, 2019.

Stallings W., *Network Security Essentials Applications and Standards*, Pearson, England 2017.

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem,* Wolters Kluwer Polska, Warszawa 2010.

Szafranek D., *Wpływ rozwoju cyberprzestępczości na funkcjonowanie współczesnych organizacji*, „Nowoczesne Systemy Zarządzania" 2021, z. 16.

Urbańska N., *Cyberprzestępczość i wynikające z niej zagrożenia,* Akademia Marynarki Wojennej, Gdynia 2025.

Zbrojewska M., *Jak definiujemy cyberprzestępstwo?*, „IAPGOŚ" 2016, 2.

Prawodawstwo

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z dnia 28.08.2014 r.).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn. Dz.U. z 2025 r. poz. 1872).

Netografia

https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=pl

Parlament Europejski, *Dlaczego cyberbezpieczeństwo jest ważne i jakie są koszty cyberataków?* https://www.europarl.europa.eu/topics/pl/article/20211008STO14521/dlaczego-cyberbezpieczenstwo-jest-wazne-i-jakie-sa-koszty-cyberatakow

EuroCert, *Atak na EuroCert – oświadczenie*, https://eurocert.pl/atak-na-eurocert-oswiadczenie/

CyberDefense24, *Co ujawnia analiza ataku na EuroCert? Ponad 100 polskich instytucji pod lupą,* https://cyberdefence24.pl/cyberbezpieczenstwo/co-ujawnia-analiza-ataku-na-eurocert-ponad-100-polskich-instytucji-pod-lupa

Kacper MAZUREK[1]

GENEZA I ISTOTA KONFLIKTU MIĘDZY STANAMI ZJEDNOCZONYMI I IZRAELEM A IRANEM

Celem rozdziału jest analiza genezy i istoty konfliktu między Stanami Zjednoczonymi i Izraelem a Iranem w ujęciu historyczno-politycznym. Wskazano kluczowe wydarzenia, takie jak przewrót w Iranie z 1953 roku, rewolucja islamska z 1979 roku oraz kryzys zakładników, które doprowadziły do trwałego pogorszenia relacji z USA. Omówiono również zmianę stosunków Iranu z Izraelem, od pragmatycznej współpracy do rywalizacji strategicznej oraz znaczenie programu nuklearnego jako głównego obszaru napięć. Zwrócono uwagę na regionalny charakter konfliktu, przejawiający się w działaniach pośrednich i presji polityczno-militarnej. Wnioskiem jest, że konflikt ma charakter długotrwały i wielowymiarowy, a jego rozwiązanie utrudniają sprzeczne interesy oraz brak wzajemnego zaufania.

Słowa kluczowe: bezpieczeństwo, konflikt, Bliski Wschód, Iran, Izrael, Stany Zjednoczone.

Wprowadzenie

Relacje między Stanami Zjednoczonymi, Izraelem i Iranem należą do najbardziej złożonych i długotrwałych napięć politycznych na Bliskim Wschodzie. Ich współczesny kształt nie jest wynikiem jednego wydarzenia, lecz splotu procesów historycznych, ideologicznych i strategicznych, które stopniowo przekształciły dawną współpracę w trwałą konfrontację. Źródła tego antagonizmu sięgają połowy XX wieku, kiedy to interesy mocarstw zaczęły coraz wyraźniej przecinać się z ambicjami regionalnymi Iranu.

Za jeden z najważniejszych punktów zwrotnych uznaje się przewrót z 1953 roku, kiedy to amerykańskie służby odegrały istotną rolę w obaleniu rządu Mohammada Mosaddegha, co w irańskiej pamięci zbiorowej stało się symbolem zewnętrznej ingerencji i poczucia niesprawiedliwości. Wydarzenie to nie tylko przywróciło władzę szachowi, ale również zapoczątkowało długotrwałą niechęć do Stanów Zjednoczonych jako państwa ingerującego w suwerenność Iranu. W kolejnych dekadach wspieranie przez USA autorytarnego reżimu szacha, modernizującego kraj w duchu zachodnim, lecz jednocześnie represyjnego wobec opozycji, pogłębiało społeczne niezadowolenie i wzmacniało nastroje antyamerykańskie. W tym okresie Izrael, blisko współpracujący z szachem w zakresie

[1] Kacper Mazurek, student Politechniki Rzeszowskiej im. Ignacego Łukasiewicza, Koło Naukowe Polityki Bezpieczeństwa Państwa. ORCID: 0009-0002-0818-7407.

bezpieczeństwa i wywiadu, również zaczął być postrzegany jako element Zachodniego bloku ingerującego w sprawy regionu[2].

Kolejnym kluczowym momentem była rewolucja islamska z 1979 roku, która nie tylko obaliła prozachodni reżim szacha, lecz także nadała polityce Iranu wyraźnie antyamerykański i antyizraelski charakter. Nowe władze, kierowane przez ajatollaha Chomeiniego, zbudowały swoją legitymizację na sprzeciwie wobec Zachodu, co przełożyło się na ideologiczne odrzucenie dotychczasowych sojuszy i redefinicję miejsca Iranu w regionie. Izrael, dotąd postrzegany jako partner strategiczny, został uznany za wrogi element prozachodni i przeciwnika religijno-politycznego, a USA za głównego wroga rewolucji. Zmiana ta miała charakter nie tylko polityczny, lecz również symboliczny, ponieważ stała się fundamentem nowej tożsamości państwowej Iranu[3].

Kulminacją narastającej wrogości stał się kryzys zakładników w ambasadzie USA w Teheranie, który definitywnie zerwał dawny model relacji irańsko-amerykańskich i ugruntował wzajemną nieufność. Trwające 444 dni przetrzymywanie amerykańskich dyplomatów stało się jednym z najbardziej dramatycznych epizodów w historii stosunków obu państw, a w USA wywołało głębokie poczucie upokorzenia i zagrożenia. W Iranie natomiast wydarzenie to zostało przedstawione jako symboliczne zwycięstwo nad imperializmem Zachodu, co na trwałe zakorzeniło antyamerykańską retorykę w polityce wewnętrznej i zagranicznej. Kryzys ten nie tylko zamroził relacje dyplomatyczne, ale również stworzył podłoże pod późniejsze konflikty dotyczące programu nuklearnego, sankcji oraz rywalizacji o wpływy w regionie[4].

Warto więc zwrócić uwagę na to, w jaki sposób dawne doświadczenia polityczne, rywalizacja o wpływy regionalne oraz spór o program nuklearny doprowadziły do utrwalenia się obecnej architektury napięć. Istotne znaczenie ma tu również fakt, że konflikt nie ogranicza się do relacji dwustronnych. W praktyce obejmuje on także bezpieczeństwo regionalne, system sankcji, politykę odstraszania oraz działania pośrednie prowadzone poprzez sojuszników i grupy zbrojne. W związku z tym napięcie to pozostaje jednym z kluczowych punktów zapalnych na Bliskim Wschodzie.

Historyczne źródła antagonizmu irańsko-amerykańskiego

Geneza konfliktu między Stanami Zjednoczonymi a Iranem nie sprowadza się do jednego kryzysu, lecz do narastania wzajemnej nieufności, która z czasem stała się trwałym elementem polityki obu państw. Punktem zwrotnym był przewrót

[2] M. Fatalski, *US Intervention in Iran (1951–1953)*, "Ad Americam" 2005, nr 6, s. 1–10.
[3] M. Furlan, *Israeli-Iranian relations: past friendship, current hostility*, "Israel Affairs" 2022, t. 28, nr 2, s. 170–172.
[4] European Pulse, *444 DAYS THAT SHOOK THE WORLD! The American hostage crisis in Tehran*, "European Pulse", https://europeanpulse.eu/pl/politics/444-days-that-shocked-the-world-the-american-hostage-crisis-in-tehran/ (dostęp: 18.04.2026 r.).

z 1953 roku przeciwko rządowi Mohammada Mosaddegha[5]. Operacja TPAJAX była przygotowywana i prowadzona w sposób systemowy, a prezydent Dwight Eisenhower wprost odnosił się później do roli USA w obaleniu Mosaddegha i przywróceniu szacha do władzy. W irańskiej pamięci politycznej wydarzenie to utrwaliło obraz Ameryki jako mocarstwa skłonnego do ingerencji w sprawy wewnętrzne Iranu, gdy wymagały tego interesy strategiczne Zachodu[6].

Skutkiem przewrotu było umocnienie monarchii szachowskiej oraz jej silniejszego związania z USA. Zakładano, że amerykańska pomoc wojskowa wzmocni prestiż szacha, utrwali prozachodni kierunek polityki Iranu i zwiększy jego zdolność do utrzymania wewnętrznej stabilności. Taki model relacji opierał się na połączeniu wsparcia militarnego, politycznego i strategicznego. Z jednej strony wzmacniał on państwo Irańskie w logice zimnowojennej, z drugiej jednak strony pogłębiał społeczne przekonanie, że elita rządząca opiera swoją pozycję na zewnętrznym protektoracie, a nie na własnej legitymizacji. W tym sensie przewrót z 1953 roku stał się nie tylko wydarzeniem politycznym, lecz także długofalowym źródłem antyamerykańskiego resentymentu.

Drugim wielkim momentem była rewolucja islamska z 1979 roku, która zniosła dawny porządek monarchiczny i otworzyła nowy etap w relacjach z Waszyngtonem. Kryzys zakładników w ambasadzie USA w Teheranie, rozpoczęty 4 listopada 1979 roku, nadał temu konfliktowi wymiar symboliczny i emocjonalny[7]. Wówczas to ponad 50 Amerykanów zostało uwięzionych na 444 dni, a sam epizod poważnie osłabił politykę zagraniczną administracji Cartera. W praktyce oznaczało to przejście od napiętej współpracy i zależności do trwałej wrogości, w której obie strony zaczęły postrzegać się jako zagrożenie dla własnych interesów bezpieczeństwa i własnej tożsamości politycznej. Od tego momentu antagonizm przestał mieć charakter incydentalny, a stał się trwałą cechą relacji dwustronnych[8].

Istotnym elementem tej genezy była również regionalna pozycja Iranu i jego relacje z Izraelem przed 1979 rokiem. Iran utrzymywał kontakty handlowe i polityczne z Izraelem, a irańska ropa trafiała tam od 1957 roku, choć nierzadko za pośrednictwem podmiotów trzecich. W czasie kryzysu bliskowschodniego z 1967 roku Teheran próbował jednocześnie utrzymywać relacje z Izraelem i nie zrywać więzi z częścią państw arabskich. Po rewolucji sytuacja uległa zasadniczej zmianie, Iran zaczął postrzegać Izrael jako element wrogiego ładu regionalnego, a spór

[5] Mohammad Mosaddegh – irański polityk, doktor prawa, uczestnik rewolucji konstytucyjnej, deputowany, minister i gubernator kilku prowincji. Demokratycznie wybrany premier Iranu, urzędujący w latach 1951–1953, z krótką przerwą w 1952 r. Inicjator nacjonalizacji irańskich zasobów ropy naftowej. Podejrzewany przez rządy Stanów Zjednoczonych i Wielkiej Brytanii o skłonności komunistyczne, został obalony w zorganizowanym przez CIA i MI6 wojskowym zamachu stanu w 1953 r. Resztę życia spędził w uwięzieniu.

[6] A. Magliocca, A. Pellegrino, J.L. Adragna, *Operation TPAJAX: An Investigation into the 1953 Iranian Coup d'État*, "Social Education" 2019, t. 83, nr 1, s. 3-42.

[7] European Pulse, *444 DAYS…,* dz. cyt.

[8] M. Bonakdarian, *U.S.-Iranian Relations, 1911–1951* [w:] *The United States and the Middle East. Diplomatic and Economic Relations in Historical Perspective*, "Yale" 2000, s. 9-21.

z USA coraz mocniej splatał się z rywalizacją o bezpieczeństwo na Bliskim Wschodzie. Właśnie dlatego konflikt amerykańsko-irański nie jest wyłącznie sporem bilateralnym, lecz częścią szerszej układanki regionalnej, w której kwestia izraelska stała się jednym z głównych punktów zapalnych[9].

Do historycznej nieufności doszedł później jeszcze wymiar nuklearny, który nadał konfliktowi nową jakość i uczynił go problemem trwałym, a nie jedynie politycznym epizodem. IAEA prowadzi dziś osobną, specjalną stronę poświęconą monitoringowi i weryfikacji w Iranie, co pokazuje, że sprawa programu jądrowego pozostaje jednym z centralnych obszarów międzynarodowej kontroli i sporów interpretacyjnych[10]. Z perspektywy historyczno-politycznej oznacza to, że antagonizm między USA a Iranem wyrósł z połączenia trzech procesów: ingerencji z 1953 roku, rewolucji i kryzysu zakładników z 1979 roku oraz stopniowej regionalizacji sporu, w której znaczenie zyskały relacje z Izraelem i kwestia bezpieczeństwa nuklearnego. To właśnie ta kumulacja nadaje konfliktowi jego długotrwały i wielowarstwowy charakter.

Izrael jako drugi biegun konfliktu

W relacjach irańsko-izraelskich najistotniejsze jest to, że przed 1979 rokiem nie miały one jeszcze charakteru otwarcie wrogiego. Porozumienie między Iranem a Izraelem było przez lata dość stabilne i opierało się przede wszystkim na wspólnym sprzeciwie wobec arabskiego nacjonalizmu oraz na zbieżności interesów wobec Iraku. W latach 50. i 60. oba państwa utrzymywały kontakty polityczne i gospodarcze, a ich relacje miały charakter pragmatyczny, a nie ideologiczny. W praktyce Izrael był dla szacha jednym z instrumentów równoważenia wpływów regionalnych, natomiast Iran pozostawał dla Izraela ważnym partnerem w otoczeniu zdominowanym przez państwa arabskie[11].

Taki układ zaczął się rozpadać wraz z rewolucją islamską. Upadek monarchii Pahlawich[12] i ustanowienie Republiki Islamskiej oznaczały nie tylko zmianę ustroju, ale także całkowitą przebudowę polityki zagranicznej. Rewolucja z lat 1978–1979 była odpowiedzią na autokrację szacha, wpływy Zachodu, kryzysy społeczne i represje polityczne, a po jej zwycięstwie w Iranie ukształtował się system otwarcie antyzachodni. W tym nowym porządku Izrael przestał być

[9] M. Furlan, *Israeli-Iranian relations…,* dz. cyt., s. 170-179.

[10] IAEA, *IAEA and Iran – IAEA Board Reports*, "IAEA", https://www.iaea.org/newscenter/focus/iran/iaea-and-iran-iaea-board-reports (dostęp: 18.04.2026 r.).

[11] J. Dryden, *Iran, Israel, and the Struggle for the Skies over the Middle East*, "Æther: A Journal of Strategic Airpower & Spacepower" 2023, t. 2, nr 1, s. 86-88.

[12] Upadek monarchii (dynastii) Pahlawich – spowodowany przez narastające niezadowolenie społeczne z autorytarnego stylu rządów, rosnących nierówności oraz brutalnych działań służb bezpieczeństwa, co połączyło różne grupy społeczne przeciwko szachowi. Jej obalenie doprowadziło do głębokiej przebudowy ustroju, zastąpienia monarchii systemem teokratycznym, podporządkowania instytucji państwowych duchowieństwu oraz istotnego ograniczenia swobód obywatelskich i pluralizmu politycznego.

postrzegany jako pragmatyczny partner, a zaczął być traktowany jako element szerszego układu sił wspieranego przez USA. Zmiana ta miała więc charakter strukturalny. Dotyczyła nie tylko stosunków dwustronnych, lecz także całej irańskiej definicji bezpieczeństwa regionalnego[13].

Po 1979 roku konflikt z Izraelem nabrał w Iranie również wymiaru symbolicznego. Wydarzenia z lat 1973–1979, czyli Wojna Jom Kippur[14] i wynikające z niej kryzysy naftowe oraz rosnące powiązanie polityczne USA z Izraelem stworzyły regionalny kontekst, w którym rewolucyjna elita mogła budować swoją legitymizację na hasłach antyimperialistycznych. Zajęcie ambasady USA i kryzys zakładników stały się wyrazistym zerwaniem z dotychczasowym porządkiem, a Izrael zaczął być postrzegany nie tylko jako przeciwnik polityczny, lecz także jako symbol amerykańskiej obecności na Bliskim Wschodzie[15]. To właśnie dlatego spór irańsko-izraelski nie ogranicza się do klasycznej rywalizacji między dwoma państwami, a ma on także wymiar ideologiczny, w którym przeciwnik jest definiowany jako część szerszego, wrogiego ładu regionalnego. Tę interpretację wzmacnia fakt, że po rewolucji Iran konsekwentnie odrzucał dawną logikę współpracy z Izraelem, zastępując ją retoryką oporu i konfrontacji.

Warto jednak zauważyć, że konflikt ten nie miał od razu formy bezpośredniej wojny. Długo rozwijał się raczej jako rywalizacja pośrednia, w której znaczenie miały sojusze, presja dyplomatyczna, wsparcie dla partnerów regionalnych i spór o wpływy. Z perspektywy historyczno-politycznej można więc uznać, że Izrael stał się drugim biegunem konfliktu wtedy, gdy relacje Iranu z USA zostały już trwale zerwane, a spór o bezpieczeństwo Bliskiego Wschodu zaczął obejmować także wymiar izraelski. Oznaczało to przejście od dawnego partnerstwa taktycznego do długotrwałej konfrontacji strategicznej, która do dziś pozostaje jednym z głównych elementów polityki Iranu wobec Zachodu i regionu.

Program nuklearny Iranu oraz narastanie presji USA i Izraela

Kwestia programu nuklearnego Iranu stała się jednym z najważniejszych elementów konfliktu Iranu z USA i Izraelem, ponieważ połączyła w sobie problem bezpieczeństwa regionalnego, kontroli zbrojeń i wzajemnej nieufności politycznej. W praktyce nie chodziło wyłącznie o same technologie jądrowe, lecz o pytanie, czy Iran dąży do uzyskania potencjału militarnego, który mógłby zmienić układ sił

[13] M. Furlan, *Israeli-Iranian relations…,* dz. cyt., s. 170.

[14] Wojna Jom Kippur – konflikt zbrojny, który wybuchł w październiku 1973 roku, gdy Egipt i Syria niespodziewanie zaatakowały Izrael, próbując odzyskać terytoria utracone w 1967 roku. Walki szybko przerodziły się w kryzys międzynarodowy, angażując mocarstwa i prowadząc do pierwszego globalnego kryzysu naftowego, ponieważ państwa arabskie ograniczyły eksport ropy do krajów wspierających Izrael. Konflikt znacząco zmienił układ sił na Bliskim Wschodzie i pokazał, jak silnie regionalne wojny mogą wpływać na gospodarkę światową.

[15] M. Furlan, *Israeli-Iranian relations…,* dz. cyt., s. 170-174.

na Bliskim Wschodzie. Tak więc spór o Iran od początku miał także wymiar instytucjonalny i kontrolny.

Za moment przełomowy uznaje się ujawnienie w 2002 roku niezgłoszonych wcześniej instalacji w Natanz i Araku. Irańska opozycja ujawniła wówczas istnienie tych obiektów, a pierwsze raporty z 2003 roku sporządzone przez International Atomic Energy Agency, czyli agencji zajmującej się bezpiecznym, pokojowym i nadzorowanym wykorzystaniem energii jądrowej potwierdziły, iż Iran budował zakłady wzbogacania uranu w Natanz oraz ciężkowodny reaktor w Araku, przy czym nie wywiązał się w pełni ze zobowiązań wynikających z układu safeguards. Z punktu widzenia USA i Izraela nie był to jedynie techniczny problem deklaracyjny, ale sygnał, że Iran rozwija infrastrukturę o znaczeniu strategicznym poza pełną kontrolą międzynarodową[16].

W kolejnych latach narastała presja dyplomatyczna i sankcyjna. Rada Bezpieczeństwa ONZ w rezolucji 2231 z 2015 roku[17] zatwierdziła Joint Comprehensive Plan of Action (JCPOA), a sama rezolucja była postrzegana przez ONZ jako fundamentalna zmiana w podejściu do irańskiej kwestii nuklearnej. Jej logika polegała na tym, że pełne wdrożenie porozumienia miało zwiększyć zaufanie do pokojowego charakteru irańskiego programu, a w zamian przewidywano stopniowe wygaszanie wcześniejszych sankcji ONZ. Innymi słowy, presja nie miała charakteru wyłącznie karzącego, lecz miała doprowadzić do ograniczenia programu i jego większej przejrzystości.

Porozumienie z 2015 roku nie zakończyło jednak sporu, lecz jedynie go czasowo uporządkowało. IAEA od 16 stycznia 2016 roku do 8 maja 2019 roku monitorowała wdrażanie przez Iran zobowiązań nuklearnych wynikających z JCPOA, natomiast po wycofaniu się Stanów Zjednoczonych w maju 2018 roku sytuacja zaczęła się pogarszać. Od 8 maja 2019 roku Iran stopniowo przestawał realizować swoje zobowiązania, a od 23 lutego 2021 roku całkowicie zaprzestał wykonywania części z nich, w tym związanych z Additional Protocol[18]. Oznaczało to także ograniczenie dostępu Agencji do kluczowych działań weryfikacyjnych.

Tak więc konflikt nuklearny stał się polem nacisku politycznego, a nie wyłącznie negocjacji technicznych. Wraz z wycofaniem USA z JCPOA wzrosło znaczenie sankcji jako narzędzia nacisku, natomiast w Iranie umocniło się przekonanie, że porozumienie nie gwarantuje trwałej normalizacji relacji z Waszyngtonem. IAEA nadal publikuje osobne materiały poświęcone monitorowaniu Iranu, co samo w sobie dowodzi, że problem nie został rozwiązany, lecz jedynie utrzymywany w ramach międzynarodowej kontroli[19].

---

[16] M. Soltaninejad, *Iran's Nuclear Policy: A Cognitive Study on Defiance and Compliance*, "Central European Journal of International and Security Studies" 2023, t. 17, nr 1, s. 7-9.

[17] United Nations Security Council Resolution 2231 (2015).

[18] Y. Gunawan, A.A.P. Riyanto, W.S. Putri, C. Asela, D. Irrynta, *Should the JCPOA be Revived? An Analysis of the Iran Nuclear Deal*, "Jurnal Nurani Hukum" 2022, t. 5, nr 2, s. 97-103.

[19] M. Rhodes, *Iran's Nuclear Program: U.S. Options After the Elections*, "Connections: The Quarterly Journal" 2005, t. 4, nr 2, s. 93-98.

W przypadku Izraela program nuklearny Iranu od dawna był postrzegany jako zagrożenie egzystencjalne. Izrael traktuje irańskie ambicje nuklearne jako bezpośrednie zagrożenie dla swojego bezpieczeństwa i preferuje rozwiązania prewencyjne, w tym działania militarne oraz operacje skryte. Taki sposób myślenia wynika z szerszej doktryny bezpieczeństwa Izraela, w której niedopuszczenie do powstania wrogiego potencjału nuklearnego jest uznawane za nadrzędny cel strategiczny. W tym sensie presja na Iran nie była wyłącznie reakcją na kolejne raporty IAEA, ale także konsekwencją izraelskiej percepcji zagrożenia[20].

Właśnie dlatego program nuklearny stał się osią wspólnej presji USA i Izraela, choć ich instrumenty nie zawsze były identyczne. Stany Zjednoczone częściej wykorzystywały negocjacje, sankcje i wielostronne mechanizmy prawne, podczas gdy Izrael akcentował możliwość prewencji militarnej i sabotażu. Oba państwa łączyło jednak przekonanie, że nawet ograniczony postęp Iranu w dziedzinie wzbogacania uranu zmienia równowagę sił na Bliskim Wschodzie. Rezolucja 2231, system IAEA oraz późniejsze załamanie się pełnej współpracy Iranu z tą agencją pokazują, że spór o program nuklearny stał się trwałym elementem konfliktu polityczno-strategicznego, a nie jedynie przejściowym kryzysem dyplomatycznym.

Wojny zastępcze, sankcje i równowaga sił na Bliskim Wschodzie

W ostatnich dekadach konflikt USA i Izraela z Iranem przestał być jedynie sporem dwustronnym i stał się zjawiskiem regionalnym, rozgrywanym poprzez sojuszników, grupy pośrednie i presję na kluczowe szlaki komunikacyjne. Jednym z najważniejszych narzędzi irańskiej polityki jest rozbudowana sieć milicji i ugrupowań współpracujących z Teheranem, działających od Libanu po Jemen i umożliwiających Iranowi projekcję siły przy jednoczesnym ściągnięciu z siebie odpowiedzialności za ich działania. Z perspektywy Iranu taki model pozwala zwiększać wpływy bez wchodzenia w bezpośrednią wojnę z silniejszym przeciwnikiem, a zarazem wiąże bezpieczeństwo państwa z losami całego regionu[21].

Regionalizacja konfliktu szczególnie wyraźnie ujawniła się po wybuchu wojny między Izraelem a Hamasem[22] w październiku 2023 roku, kiedy to po tym wydarzeniu wspierane przez Iran grupy nasiliły ataki na cele amerykańskie i izraelskie w Iraku oraz Syrii, a Stany Zjednoczone odpowiedziały uderzeniami na

[20] F. Jahanpour, *Iran's Nuclear Programme and Regional Security*, "Oxford Research Group" 2007, s. 1-7.

[21] A.J. Watkins, *The Future of Iran's Influence Through Proxy Employment*, "Naval Postgraduate School", Monterey, 2021, s. 13-26.

[22] Hamas – inaczej Muzułmański Ruch Oporu, to islamska sunnicka i fundamentalistyczna organizacja polityczno-militarna walcząca o niepodległość Palestyny i uznawana przez państwa zachodnie za terrorystyczną.

obiekty powiązane z Iranem. W tym samym czasie Hezbollah[23] w Libanie i Huti[24] w Jemenie dołączyli do presji na Izrael i na amerykańską obecność w regionie, co unaoczniło, że konflikt irańsko-amerykański nie ma jednego frontu, lecz rozgałęzia się na kilka teatrów jednocześnie. W praktyce oznaczało to ryzyko rozszerzenia wojny poza pierwotny obszar starcia[25].

Istotne jest również to, że Iran od lat buduje swoją pozycję w logice asymetrycznej. Sieć proxy stanowi dla Teheranu nie tylko narzędzie nacisku, ale także mechanizm obrony własnego reżimu i źródło strategicznej głębi. Wspieranie ugrupowań takich jak Hezbollah, część milicji irackich czy Huti umożliwia Iranowi oddziaływanie na decyzje przeciwników, rozpraszanie ich zasobów i przenoszenie kosztów konfliktu poza własne terytorium. Z punktu widzenia USA i Izraela jest to szczególnie problematyczne, ponieważ każda eskalacja może obejmować jednocześnie bezpieczeństwo lądowe, morskie i powietrzne[26].

Regionalny wymiar konfliktu obejmuje także bezpieczeństwo żeglugi i kluczowych cieśnin. Iran jest w stanie zagrozić przepływom w cieśninie Ormuz, która łączy Zatokę Perską z Oceanem Indyjskim. Nawet krótkotrwałe zakłócenia w tym rejonie mają znaczenie nie tylko wojskowe, ale też gospodarcze, ponieważ wpływają na ceny energii i stabilność handlu międzynarodowego. Z tego powodu konflikt z Iranem nigdy nie ogranicza się do sporu ideologicznego, a dotyka także globalnej infrastruktury bezpieczeństwa i rynku surowców.

Ważną rolę odgrywa również presja sankcyjna, która od lat pozostaje podstawowym narzędziem USA wobec Teheranu. Choć sankcje mają osłabiać zdolność Iranu do finansowania programu nuklearnego i sieci regionalnych wpływów, w praktyce często wzmacniają logikę konfrontacji. Iran interpretuje je jako próbę ekonomicznego zduszenia państwa i wymuszenia zmiany jego polityki zagranicznej, podczas gdy Waszyngton i Jerozolima traktują je jako środek ograniczania potencjału militarnego i destabilizującej aktywności Iranu. W efekcie sankcje nie zamykają konfliktu, lecz utrwalają jego długotrwały charakter i wzmacniają przekonanie, że spór toczy się jednocześnie na poziomie gospodarki, dyplomacji i bezpieczeństwa.

Regionalizacja konfliktu widoczna jest także w tym, że każde większe starcie między Iranem a Izraelem czy USA pociąga za sobą reakcje łańcuchowe. W 2024 roku napięcie przeszło od działań pośrednich do bezpośredniej wymiany uderzeń, a izraelskie ataki na cele w Iranie i irańska odpowiedź rakietowo-dronowa pokazały, jak łatwo spór może wykroczyć poza pierwotne ograniczenia. Konflikt

[23] Hezbollah – libańska partia polityczna radykalnych szyitów utworzona w 1982 roku. Od początku była wspierana i finansowana przez Iran, Syrię, a także przez dotacje jej zwolenników. Organizacja określa siebie jako antyimperialistyczną.

[24] Huti – zbrojna część ruchu znanego jako Ansar Allah (Wyznawcy Allaha), jest to jemeński ruch o charakterze polityczno-militarnym, skupiający plemiona zajdyckie (jeden z odłamów szyizmu) zamieszkujące w większości północno-zachodni Jemen.

[25] A. Raghuraman, D. Mamasoliev, *Iran's Proxy Network Strategy in the Middle East*, "IAIS Research Nexus", 2005 t. 1, nr 4, s. 6-7.

[26] A.J. Watkins, *The Future…,* dz. cyt., s. 13-16.

regionalny nie jest więc dodatkiem do sporu USA i Izraela z Iranem, lecz jego podstawowym sposobem funkcjonowania.

Podsumowanie

Konflikt USA i Izraela z Iranem ma charakter długotrwały i wielowymiarowy, ponieważ jego fundamenty zostały ukształtowane przez wydarzenia historyczne, które do dziś determinują sposób postrzegania zagrożeń przez wszystkie strony. Przewrót z 1953 roku, rewolucja islamska z 1979 roku oraz kryzys zakładników stworzyły trwałą podstawę wzajemnej nieufności między Iranem a Stanami Zjednoczonymi. Równocześnie transformacja relacji Iranu z Izraelem, od pragmatycznej współpracy do otwartej wrogości spowodowała, że konflikt nabrał wymiaru regionalnego i ideologicznego, wykraczając poza klasyczne ramy stosunków bilateralnych.

W kolejnych dekadach kluczowym obszarem napięcia stał się program nuklearny Iranu, który w ocenie USA i Izraela stanowi potencjalne zagrożenie dla równowagi sił na Bliskim Wschodzie. Mechanizmy kontroli prowadzone przez IAEA oraz próby regulacji tego problemu, w tym porozumienie JCPOA, nie doprowadziły do trwałej deeskalacji. Ograniczone zaufanie między stronami oraz rozbieżne interpretacje zobowiązań przyczyniły się do wzrostu napięć i utrwalenia konfliktu jako elementu strukturalnego stosunków międzynarodowych.

Współcześnie konflikt ten uległ dalszej eskalacji i regionalizacji. Ostatnie wydarzenia na Bliskim Wschodzie, w tym bezpośrednie uderzenia między Iranem a Izraelem oraz nasilone działania grup powiązanych z Teheranem, wskazują na przejście od konfliktu pośredniego do bardziej otwartej konfrontacji. Wzrost aktywności militarnej, w tym wykorzystanie rakiet i dronów, zwiększa ryzyko niekontrolowanej eskalacji, która może objąć kolejne państwa regionu. Stany Zjednoczone jako główny sojusznik Izraela pozostają zaangażowane zarówno militarnie, jak i politycznie, co dodatkowo podnosi poziom napięcia[27].

Obecna dynamika konfliktu niesie ze sobą szereg potencjalnych konsekwencji. W krótkiej perspektywie najważniejsze jest ryzyko rozszerzenia działań zbrojnych na większą skalę, w tym możliwość bezpośredniej konfrontacji między Iranem a Izraelem z udziałem USA. Taki scenariusz mógłby doprowadzić do destabilizacji całego regionu, zakłócenia szlaków energetycznych, zwłaszcza w rejonie Zatoki Perskiej oraz wzrostu cen surowców na rynkach światowych. W dłuższej perspektywie konflikt może prowadzić do dalszej militaryzacji regionu, wzrostu znaczenia aktorów niepaństwowych oraz pogłębiania podziałów politycznych na Bliskim Wschodzie.

Nie można również wykluczyć scenariusza odwrotnego, w którym narastająca eskalacja skłoni strony do powrotu na ścieżkę negocjacji, zwłaszcza w kwestii

[27] S. Palczewski, *Wojna na Bliskim Wschodzie. Iran, Izrael i USA – operacje, których nie widać*, "CyberDefence24", https://cyberdefence24.pl/armia-i-sluzby/wojna-na-bliskim-wschodzie-iran-izrael-i-usa-operacje-ktorych-nie-widac (dostęp: 08.04.2026 r.).

programu nuklearnego. Jednak dotychczasowe doświadczenia wskazują, że nawet ewentualne porozumienia mają charakter tymczasowy i nie eliminują podstawowych źródeł konfliktu.

W związku z tym należy uznać, że konflikt USA i Izraela z Iranem pozostanie jednym z kluczowych wyzwań dla bezpieczeństwa międzynarodowego, a jego rozwój będzie zależał zarówno od decyzji politycznych głównych aktorów, jak i od dynamiki wydarzeń w regionie.

Bibliografia

Fatalski M., *US Intervention in Iran (1951–1953)*, "Ad Americam" 2005, nr 6.

Furlan M., *Israeli-Iranian relations: past friendship, current hostility*, "Israel Affairs" 2022, t. 28, nr 2.

Magliocca A., Pellegrino A., Adragna J.L., *Operation TPAJAX: An Investigation into the 1953 Iranian Coup d'État*, "Social Education" 2019, t. 83, nr 1.

Bonakdarian M., *U.S.-Iranian Relations, 1911–1951* [w:] *The United States and the Middle East. Diplomatic and Economic Relations in Historical Perspective*, "Yale" 2000.

Dryden J., *Iran, Israel, and the Struggle for the Skies over the Middle East*, "Æther: A Journal of Strategic Airpower & Spacepower" 2023, t. 2, nr 1.

Soltaninejad M., *Iran's Nuclear Policy: A Cognitive Study on Defiance and Compliance*, "Central European Journal of International and Security Studies" 2023, t. 17, nr 1.

Gunawan Y., Riyanto A.A.P., Putri W.S., Asela C., Irrynta D., *Should the JCPOA be Revived? An Analysis of the Iran Nuclear Deal*, "Jurnal Nurani Hukum" 2022, t. 5, nr 2.

Rhodes M., *Iran's Nuclear Program: U.S. Options After the Elections*, "Connections: The Quarterly Journal" 2005, t. 4, nr 2.

Jahanpour F., *Iran's Nuclear Programme and Regional Security*, "Oxford Research Group" 2007.

Watkins A.J., *The Future of Iran's Influence Through Proxy Employment*, "Naval Postgraduate School", Monterey, 2021.

Raghuraman A., Mamasoliev D., *Iran's Proxy Network Strategy in the Middle East*, "IAIS Research Nexus", 2005 t. 1, nr 4.

Prawodawstwo

United Nations Security Council Resolution 2231 (2015).

Netografia

European Pulse, *444 DAYS THAT SHOOK THE WORLD! The American hostage crisis in Tehran*, "European Pulse", https://europeanpulse.eu/pl/politics/444-days-that-shocked-the-world-the-american-hostage-crisis-in-tehran/

IAEA, *IAEA and Iran – IAEA Board Reports*, "IAEA", https://www.iaea.org/newscenter/focus/iran/iaea-and-iran-iaea-board-reports

Palczewski S., *Wojna na Bliskim Wschodzie. Iran, Izrael i USA – operacje, których nie widać*, "CyberDefence24", https://cyberdefence24.pl/armia-i-sluzby/wojna-na-bliskim-wschodzie-iran-izrael-i-usa-operacje-ktorych-nie-widac

Kacper MAZUREK[1]

KONFLIKT TRUMP–MADURO W POLITYCE STANÓW ZJEDNOCZONYCH WOBEC WENEZUELI

Opracowanie przedstawia konflikt między USA a Wenezuelą jako efekt złożonego splątania przemian wewnętrznych i zewnętrznych nacisków. Transformacji rentierskiej pod Chávezem, załamania sektora naftowego i kryzysu humanitarnego, które uczyniły reżim podatnym na presję międzynarodową. Przedstawia amerykańskie instrumenty, w tym sankcje, działania prawne, polityczną delegitymizacje władzy oraz działania konwencjonalne które na przestrzeni lat ograniczały zdolności finansowe reżimu jednocześnie pogłębiając koszty społeczne. Treść obejmuje również kulminacyjny moment będący operacją z 3 stycznia 2026 roku, w kontekście którego rozważono legalność użycia siły i immunitet głów państw.

Słowa kluczowe: bezpieczeństwo, konflikt, militarna interwencja, Stany Zjednoczone, Wenezuela.

Wprowadzenie

Konflikt między administracjami Stanów Zjednoczonych a reżimem Nicolása Maduro jest zjawiskiem zakorzenionym w długotrwałych przemianach politycznych i gospodarczych Wenezueli oraz w ewolucji amerykańskiej polityki wobec regionu. Od momentu zwycięstwa Hugo Cháveza w 1999 roku i transformacji modelu rentierskiego opierającego się na przychodach z ropy, struktura państwa w Caracas uległa głębokiej przebudowie. Instrumenty redystrybucji i klientelizmu wzmocniły pozycję władzy wykonawczej, podczas gdy zależność od eksportu surowców ograniczyła elastyczność makroekonomiczną kraju[2]. Skumulowane skutki spadku cen ropy, restrukturyzacji PDVSA oraz braku trwałych reform przełożyły się na erozję dochodów państwa i nasilenie kryzysu humanitarnego, co z kolei wpłynęło na skalę presji międzynarodowej wobec reżimu.

Polityka amerykańska wobec Caracas w ostatnich dwóch dekadach przybrała formy wielowymiarowe. Od ukierunkowanych sankcji personalnych, przez restrykcje sektorowe wobec PDVSA, aż po działania prawne i instrumenty ekonomiczne ograniczające możliwości finansowania aparatu władzy. Sankcje, choć zaprojektowane jako narzędzie nacisku na elity, wywołały także istotne skutki makrospołeczne, przyczyniając się do ekspansji gospodarki nieformalnej i kom-

[1] Kacper Mazurek, student Politechniki Rzeszowskiej im. Ignacego Łukasiewicza, Koło Naukowe Polityki Bezpieczeństwa Państwa. ORCID: 0009-0002-0818-7407.

[2] T.L. Karl, *The Paradox of Plenty: Oil Booms and Petro-States*, University of California Press, 1997, s. 15-22.

plikując kanały pomocy humanitarnej. Instrumentarium presji ma charakter hybrydowy i łączy się z działaniami dyplomatycznymi, operacjami wywiadowczymi i niekiedy planowaniem działań bardziej konwencjonalnych.

Przemiany te stworzyły tło dla eskalacji, której apogeum stanowiły wzajemne próby delegitymizacji, a następnie stosunkowo niespotykanej skali operacje z użyciem środków konwencjonalnych. Analizując konflikt USA z Wenezuelą warto połączyć perspektywę wewnętrzną z wymiarem zewnętrznym. Dopiero taka, interdyscyplinarna i wielowymiarowa rama analityczna pozwala zrozumieć genezę, przebieg i możliwe konsekwencje interwencji militarnej, której kulminacją stały się wydarzenia z początku 2026 roku, zarówno w aspekcie prawnomiędzynarodowym, jak i geopolitycznym.

Geneza konfliktu

Relacje między Waszyngtonem a Caracas mają długi i złożony rodowód, którego współczesne napięcie najlepiej rozumieć jako efekt nakładania się przemian wewnętrznych w Wenezueli i zmian w polityce zagranicznej Stanów Zjednoczonych wobec regionu. Rozpoczęte w 1999 roku przemiany spowodowane dojściem Hugo Cháveza do władzy przekształciły model polityczny i gospodarczy kraju, wprowadzając szeroką redystrybucję zasobów przy jednoczesnej koncentracji władzy w strukturach wykonawczych. Chávez wykorzystał zasoby naftowe jako fundament polityki społecznej i międzynarodowej, co z jednej strony podnosiło poparcie społeczne, a z drugiej osłabiało instytucjonalne mechanizmy kontroli państwa. To dziedzictwo nadało specyficzny charakter następnej fazie rządów, gdy po śmierci Cháveza w 2013 roku władzę przejął Nicolás Maduro[3].

Konstrukcja polityczno-gospodarcza boliwariańskiej rewolucji czyniła gospodarkę Wenezueli wyjątkowo wrażliwą na wahania cen ropy. Dominacja państwowej spółki naftowej PDVSA[4] i silne uzależnienie budżetu państwa od przychodów z eksportu surowca ograniczały zdolność adaptacyjną gospodarki wobec spadków wydobycia i rezygnacji z inwestycji. Spadek cen ropy po 2014 roku oraz brak gruntownych reform strukturalnych spowodowały gwałtowną erozję dochodów fiskalnych, co w warunkach autorytarnego zarządzania i klientelizmu przekuło się w głęboki kryzys ekonomiczny i instytucjonalny[5]. Te fundamenty gospodarcze stanowiły istotne tło dla konfliktu międzynarodowego, ponieważ osłabienie legitymacji reżimu zwiększało jego podatność na zewnętrzną presję i jednocześnie motywowało władzę do szukania sojuszników poza tradycyjnymi partnerami[6].

[3] R.D. Villa, *Venezuela: political changes in the Chávez era*, "Estudios Avanzados" 2005, s. 153-170.
[4] PDVSA – Petróleos de Venezuela, S.A., to państwowa firma naftowo-gazowa Wenezueli.
[5] H. Aray, D. Vera, *A tale of oil production collapse*, "Resources Policy" 2024, Vol. 93, s. 1-9.
[6] X.-Z. Mu, G.-W. Hu, *Analysis of Venezuela's oil-oriented economy from the perspective of entropy*, "Resources Policy" 2018, s. 1-9.

Proces erozji instytucji demokratycznych obserwowany w kolejnych latach rządów Maduro przybrał formy, które postrzegane były przez państwa zachodnie i organizacje międzynarodowe jako podważające podstawy legalności władzy. Manipulacje wyborcze, ograniczanie przestrzeni dla opozycji oraz redystrybucja kompetencji instytucji państwowych przyczyniły się do izolacji politycznej Caracas na scenie międzynarodowej. W ocenie instytucji parlamentarnych USA powyższe praktyki tworzyły przesłanki do stosowania polityki nacisku, postrzeganej jako narzędzie przywracania zasad demokratycznych lub wymuszenia zmiany rządów. W tym kontekście działania dyplomatyczne i gospodarcze skierowane przeciwko reżimowi nabrały logicznego sensu z punktu widzenia aktorów zewnętrznych dążących do powstrzymania dalszej degeneracji instytucjonalnej[7].

W kolejnych latach pojawiały się instrumenty presji pozamilitarnej. Pierwsze sankcje ukierunkowane były na osoby i podmioty powiązane z łamaniem praw człowieka i korupcją. Z czasem instrumentarium rozszerzono o restrykcje finansowe na kluczowych urzędników i ograniczenia względem transakcji państwowych. Najważniejszym przełomem okazało się wprowadzenie sankcji sektorowych wobec PDVSA i ograniczeń w dostępie do globalnych rynków finansowych, co uderzyło bezpośrednio w główne źródło przychodów państwa[8]. Skutki finansowe i operacyjne takich działań były przedmiotem licznych analiz, które wskazywały, że choć sankcje wyraźnie ograniczają możliwości finansowania aparatu władzy, to jednocześnie nasilają skutki gospodarcze i humanitarne dla ludności. Proporcjonalność i efektywność sankcji stała się jednym z kluczowych elementów oceny amerykańskiej polityki wobec Wenezueli[9].

Kryzys humanitarny i związana z nim emigracja milionów Wenezuelczyków uwidoczniły skalę tragedii społecznej, która rozgrywała się równolegle do konfliktu politycznego. Rosnące braki w zaopatrzeniu, spadek dostępności leków oraz gwałtowny spadek realnych dochodów doprowadziły do dramatycznego pogorszenia warunków życia. Nakładane pakiety sankcyjne pogłębiły istniejący kryzys. W rezultacie każdy nowy krok polityczny ze strony zewnętrznych aktorów musiał być oceniany nie tylko przez pryzmat jego wpływu na elity władzy, lecz też pod kątem kosztów społecznych[10].

Przełom polityczny nastąpił w styczniu 2019 roku, gdy wiele państw, w tym Stany Zjednoczone, uznało przewodniczącego Zgromadzenia Narodowego Juana Guaidó za tymczasowego prezydenta. Uznanie to stało się wyraźnym sygnałem zmiany strategii, ponieważ łączyło werbalne potępienie praktyk reżimu z aktywną polityką delegitymizacji oraz z próbami odcięcia reżimu od źródeł finansowania.

---

[7] R.D. Villa, *Venezuela: political...,* dz. cyt., s. 153-170.

[8] F. Monaldi, I. Hernández, J. La Rosa, *The Collapse of the Venezuelan Oil Industry*, "Center for Energy Studies" 2020, s. 36-45.

[9] B. Bull, *Into the shadows: sanctions, rentierism, and economic informalization in Venezuela*, "European Review of Latin American and Caribbean Studies Revista Europea de Estudios Latinoamericanos y del Caribe" 2020, s. 109-114.

[10] Tamże, s. 128-129.

Dla administracji amerykańskiej uznanie Guaidó funkcjonowało jako instrument legitymizacji opozycji i argument polityczny na rzecz zwiększenia nacisku. To posunięcie miało także efekt mobilizacyjny, wywołując zarówno presję wewnętrzną na elity rządowe, jak i reakcję ze strony sojuszników Maduro[11].

Równocześnie rozwój sytuacji na arenie międzynarodowej ujawnił, że konflikt nie jest wyłącznie sprawą bilateralną. Rosja, Chiny i Kuba odegrały role istotne dla przetrwania reżimu. Rosyjskie wsparcie obejmowało zarówno pomoc polityczną, jak i wsparcie techniczne i wojskowe, co zwiększało koszty interwencji i komplikowało bilans strategiczny dla państw rozważających bardziej zdecydowane działania. Chińskie inwestycje i kredyty dawały Caracas pewne pole manewru w zakresie finansowania, natomiast kubańskie wsparcie w obszarze bezpieczeństwa wewnętrznego wzmacniało zdolności represyjne reżimu. Wsparcie tych partnerów miało wymiar materialny i symboliczny, sygnalizując, że próby zewnętrznej izolacji mogą napotkać istotne przeszkody[12].

Wewnętrzna dynamika elit rządowych i sił zbrojnych pozostawała kluczowym czynnikiem decydującym o odporności reżimu. W sytuacji wysokiej presji zewnętrznej utrzymanie lojalności kluczowych grup interesu zależało od zdolności do zapewnienia korzyści materialnych i kontroli nad aparatem bezpieczeństwa. Pomimo trudności ekonomicznych reżim utrzymywał instrumenty kooptacji, które pozwalały na względną stabilizację wewnętrzną. Jednocześnie istniały znaczące napięcia wewnętrzne i potencjalne linie pęknięć[13].

Nakładanie sankcji sektorowych w połączeniu z działaniami dyplomatycznymi oraz uznaniem alternatywnych struktur władzy stworzyło środowisko, w którym retoryka dotycząca opcji użycia siły stała się znaczącym elementem kalkulacji politycznych. W praktyce to połączenie środków ekonomicznych, politycznych i militarno-strategicznych wytworzyło hybrydową formę nacisku, której skutki nie ograniczały się jedynie do zmiany równowagi sił, lecz oddziaływały na strukturę codziennego życia obywateli. W polityce zagranicznej Stanów Zjednoczonych wobec Caracas kluczowe stało się zatem pytanie o skuteczność i kosztowność zastosowanych środków oraz o ich długofalowe implikacje dla regionu. Geneza współczesnego konfliktu między administracją amerykańską a rządem madurystycznym wynika więc z nakładania się trzech głównych procesów: transformacji wewnętrznej Wenezueli pod rządami Cháveza i Maduro, kryzysu gospodarczego i humanitarnego pogłębionego przez spadki cen ropy i błędy polityki gospodarczej oraz reakcji międzynarodowej skoncentrowanej na stosowaniu narzędzi presji politycznej i ekonomicznej. Rozumienie tych procesów jest niezbędne dla późniejszej rekonstrukcji przebiegu interwencji i oceny jej konsekwencji.

---

[11] J. Galbraith, *United States Recognizes the Opposition Government in Venezuela and Imposes Sanctions as Tensions Escalate*, "American Journal of International Law" 2019, s. 601-608.

[12] U. Thoene, *Russia in Latin America: Why support Venezuela in a crisis?*, "International Social Science Journal" 2023, Vol. 73, Issue 248, s. 628-629.

[13] K. Iskandarov, *Economic coercion as a means of hybrid warfare: The South Caucasus as a focal point*, "Security and Defence Quarterly" 2022, s. 54.

Polityka Wenezueli wobec USA

Relacje Wenezueli wobec Stanów Zjednoczonych po rewolucji boliwariańskiej cechowała postawa asertywna i często konfrontacyjna, odwołująca się do retoryki suwerenności surowcowej i oporu wobec „interwencjonizmu" Waszyngtonu. Polityka ta była formą odpowiedzi na historyczne asymetrie w stosunkach gospodarczych (dominacja inwestycji i rynków amerykańskich) oraz na konkretne napięcia polityczne, które eskalowały od początku rządów Cháveza. W praktyce oznaczało to zarówno działania legislacyjne i wykonawcze wewnątrz kraju, jak i instrumenty zewnętrzne, w tym wykorzystanie państwowego sektora naftowego jako narzędzia wpływu oraz próby międzynarodowego budowania alternatywnych sojuszy.

Konkretne akty polityki gospodarczej wobec podmiotów zagranicznych przybierały formę nacjonalizacji i przejmowania kontroli nad projektami i infrastrukturą. W 2007 roku władze w Caracas przeprowadziły falę przejęć i zmian kontraktowych wobec zagranicznych koncernów naftowych, w tym firm amerykańskich, co oznaczało przymusowe przekształcenie dotychczasowych umów w przedsiębiorstwa z dominującym udziałem państwa albo bezpośrednie przejęcie aktywów. Te decyzje miały wymiar polityczny oraz ekonomiczny[14].

Motywacje rządów Cháveza, a później Maduro dla takich działań należały do kombinacji doktryny „suwerenności nad zasobami", chęci redystrybucji dochodów z sektora paliwowego na programy socjalne oraz logiki zabezpieczenia politycznego reżimu wobec realnej i postrzeganej presji zewnętrznej. Narodowe przejęcia umożliwiały Caracas kontrolę nad kluczowymi źródłami finansowania państwa, a także budowę politycznego kapitału wśród beneficjentów programów socjalnych. Równocześnie działania te służyły mobilizacji retorycznej przeciw ingerencji zewnętrznej i umacnianiu legitymizacji wewnętrznej[15].

Skutki prawne i gospodarcze tych decyzji szybko znalazły odzwierciedlenie w sporach międzynarodowych. Amerykańskie koncerny, które straciły aktywa w Wenezueli, kierowały roszczenia do trybunałów arbitrażowych i uzyskiwały orzeczenia nakazujące odszkodowania. Te spory pogłębiły antagonizmy i stworzyły długotrwałe zobowiązania finansowe oraz presję prawną wobec Caracas[16].

Równolegle Wenezuela wykorzystywała własne aktywa poza granicami jako instrument strategiczny. PDVSA poprzez swoją spółkę-córkę CITGO kontrolo-

[14] Reuters, *Chavez drives Exxon and ConocoPhillips from Venezuela*, "Reuters", https://www.reuters.com/article/business/chavez-drives-exxon-and-conocophillips-from-venezuela-idUSN26378950/?.com (dostęp: 11.02.2026 r.).

[15] P. Isbell, *Hugo Chávez and the Future of Venezuelan Oil (I): The Resurgence of Energy Nationalism (ARI)*, "Real Instituto Elcano", https://www.realinstitutoelcano.org/en/analyses/hugo-chavez-and-the-future-of-venezuelan-oil-i-the-resurgence-of-energy-nationalism-ari/?.com, (dostęp: 11.02.2026 r.).

[16] M. Parraga, *Venezuela must pay Conoco over $8 billion – World Bank*, "Reuters", https://www.reuters.com/article/world/venezuela-must-pay-conoco-over-8-billion-world-bank-idUSKCN1QP20I/?.com (dostęp: 11.02.2026 r.).

wała rafinerie i aktywa w USA, co dawało Caracas zarówno kanały eksportu, jak i narzędzia negocjacyjne. Ta asymetria (przejęcia aktywów amerykańskich firm w Wenezueli i posiadanie przez Wenezuelę istotnych aktywów w USA) komplikowała reakcję Waszyngtonu. Z jednej strony polityczne potępienie i presja, z drugiej strony praktyczne wyzwania związane z własnością i bezpieczeństwem dostaw paliw[17].

Tak więc polityka Wenezueli wobec USA była w istocie połączeniem polityki wewnętrznej, związanej z konsolidacją władzy i redystrybucją przychodów, z geopolitycznym użyciem zasobów naturalnych i aktywów międzynarodowych. Nacjonalizacje i kontrola nad sektorem naftowym miały umocnić suwerenność i źródła dochodów reżimu, lecz jednocześnie wywołały długotrwałe reperkusje prawne, ekonomiczne i polityczne, które z kolei legitymizowały ostrzejsze środki wobec Caracas ze strony Waszyngtonu.

Polityka USA wobec Wenezueli

Relacje Waszyngtonu wobec Caracas ukształtowały się w reakcji na działania władz wenezuelskich, w tym fale nacjonalizacji aktywów zagranicznych i wykorzystania sektora naftowego jako narzędzia politycznego. Obecną politykę USA wobec Wenezueli można rozumieć jako bezpośredni skutek działań rządów Cháveza i Maduro.

Pierwszą i najbardziej widoczną odpowiedzią były środki ekonomiczno-finansowe, czyli system sankcji, które z czasem rozszerzały się od kar personalnych na kluczowych urzędników do sankcji sektorowych wymierzonych w PDVSA i powiązane spółki. W styczniu 2019 roku Departament Skarbu USA, za pośrednictwem OFAC, objął PDVSA sankcjami związanymi z sektorem naftowym, co umożliwiło blokowanie transakcji i ograniczyło przepływy dochodów z ropy. Sankcje te były instrumentem presji ekonomicznej mającej zdestabilizować możliwości reżimu w zakresie finansowania władzy, lecz równocześnie rodziły dyskusje o skutkach dla obywateli i rynków globalnych[18].

Drugim kanałem odpowiedzi były działania prawne i arbitrażowe podejmowane przez amerykańskie i międzynarodowe podmioty poszkodowane przez nacjonalizacje. Sprawy takie jak arbitraż ConocoPhillips, wynikający z przejęć aktywów firmy w 2007 roku, doprowadziły do wielomiliardowych orzeczeń na korzyść koncernów, które w konsekwencji mogły egzekwować należności wobec wenezuelskich aktywów za granicą. Instrument prawny stał się zatem narzędziem odwetu

[17] Congressional Research Service, *Venezuela: Background and U.S. Relations*, "Congressional Research Service" 2022, s. 20-22.

[18] B. Bull, *Into the shadows: sanctions, rentierism, and economic informalization in Venezuela*, "European Review of Latin American and Caribbean Studies Revista Europea de Estudios Latinoamericanos y del Caribe" 2020, s. 108-129.

i mechanizmem, który wzmacniał pozycję Waszyngtonu i przedsiębiorstw amerykańskich przy próbach odzyskania wartości utraconych inwestycji[19].

Trzeci wymiar to działania polityczno-dyplomatyczne. Uznawanie alternatywnych władz, wsparcie dla opozycji i wykorzystanie legitymizacji międzynarodowej jako narzędzia presji. Najbardziej spektakularnym przykładem była decyzja administracji USA i części sojuszników o uznaniu Juana Guaidó za tymczasowego prezydenta w styczniu 2019 roku, co z jednej strony miało delegitymizować reżim Maduro, a z drugiej umożliwić transfer kontroli nad pewnymi aktywami i kanałami finansowymi w kierunku opozycji lub neutralnych zarządców. Jednakże taka polityka była jednocześnie źródłem międzynarodowej polaryzacji[20].

Czwarty element to działania praktyczne wobec aktywów zagranicznych PDVSA i jej spółek-córek, zwłaszcza CITGO. Stany Zjednoczone stosowały kombinację ochrony prawnej, licencji OFAC i czasowego zabezpieczenia aktywów, aby zapobiec ich przejęciu przez wierzycieli czy niekontrolowanym transakcjom. W pewnych momentach Waszyngton udzielał licencji mających na celu chronienie rafinerii i zapobieganie destabilizacji rynku paliwowego lub umożliwienie ograniczonych operacji humanitarnych, co ukazuje pragmatyczny wymiar polityki poprzez jednoczesne sankcjonowanie reżimu i ochronę krytycznych elementów infrastruktury[21].

Tak więc polityka USA wobec Wenezueli była złożoną i wielowymiarową prawno-ekonomiczną odpowiedzią na nacjonalizacje i instrumentalne wykorzystanie zasobów, częściową delegitymizacją polityczną reżimu oraz praktycznymi krokami wobec aktywów zagranicznych, które wymagały uregulowania i ochrony. Sankcje i działania prawne ograniczały możliwości rządu w Caracas, lecz równocześnie komplikowały kanały gospodarcze i humanitarne, powodując dylematy dotyczące kosztów społecznych oraz długoterminowej stabilności państwa.

Przygotowanie i przebieg interwencji

Interwencja USA z 3 stycznia 2026 roku była poprzedzona wcześniejszymi przygotowaniami, a sama nie stanowiła pierwszej próby porwania Nicolása Maduro. Z tego względu należ przeanalizować całość działań i wydarzeń, których punktem kulminacyjnym była interwencja USA.

Warto wpierw zwrócić uwagę na próbę z 2020 roku, znaną jako Operation Gideon, która stanowiła próbę zamachu stanu przez wenezuelską opozycję, przeprowadzoną z pomocą prywatnych najemników ze Slivercorp USA. Atak zakładał

[19] M. Parraga, *Venezuela must pay Conoco over $8 billion – World Bank*, "Reuters", https://www.reuters.com/article/world/venezuela-must-pay-conoco-over-8-billion-world-bank-idUSKCN1QP20I/?.com (dostęp: 11.02.2026 r.).

[20] J. Galbraith, *United States Recognizes the Opposition Government in Venezuela and Imposes Sanctions as Tensions Escalate*, "American Journal of International Law" 2019, s. 601-608.

[21] Reuters, *US extends protection of Venezuela-owned Citgo from creditors*, "Reuters", https://www.reuters.com/business/energy/us-extends-protection-venezuela-owned-citgo-creditors-2026-02-02/?.com (dostęp: 11.02.2026 r.).

wpłynięcie łodzią do portu Macuto od 3 do 4 maja 2020 roku w celu przejęcia kontroli nad lotniskiem międzynarodowym im. Simóna Bolívara w Maiquetii, zatrzymania Nicolasa Maduro i innych wysokich rangą osobistości w jego rządzie oraz wydalenia ich z kraju. Operacja została jednak wykryta przez funkcjonariuszy służb specjalnych rządu Maduro i tym samym zakończyła się porażką i ujęciem jej uczestników, natomiast samemu reżimowi przysporzyła materiału propagandowego. Ten epizod ujawnił dwa ważne wnioski dla późniejszych planów porwania prezydenta Wenezueli. Po pierwsze, że operacje z użyciem prywatnych kontraktorów niosą wysokie ryzyko kompromitacji i ofiar. Po drugie, że istniały kanały i osoby gotowe dostarczać informacje o ruchach władz Maduro. Ten precedens wpłynął na decyzję, by w kolejnych latach część działań przenieść pod kontrolę państwową i poprzeć je rozbudowaną pracą wywiadowczą oraz prawną[22].

Niezwykle istotne było także narastające użycie instrumentów prawnych i nagród motywacyjnych, które w latach 2024–2025 przybrały wyraźną formę. Władze USA systematycznie formułowały zarzuty wobec członków otoczenia Maduro i stopniowo zwiększały presję dyplomatyczną. Kluczowym momentem było podwyższenie nagrody za informacje prowadzące do zatrzymania Nicolása Maduro do 50 mln USD, co miało zmobilizować źródła i równocześnie wzmocnić podstawy prawne ewentualnych działań egzekucyjnych. Ten element „prawno-publiczny" pełnił rolę zarówno narzędzia gromadzenia informacji, jak i legitymizacji dalszych kroków wobec reżimu[23].

Równolegle do działań prawnych nasiliła się presja ekonomiczna i logistyczna, szczególnie operacje przeciw tzw. shadow fleet oraz sankcje wymierzone w PDVSA. Od połowy 2025 roku USA i ich partnerzy zintensyfikowali śledzenie oraz w pewnych przypadkach przejmowanie tankowców podejrzanych o omijanie embarga, co realnie ograniczało przepływy finansowe reżimu. Ten etap działania miał charakter przygotowawczy. Poprzez przecięcie kanałów dochodów osłabiano zdolność władz do długotrwałego odpierania nacisków i równocześnie tworzono „okno" operacyjne dla działań bardziej konwencjonalnych[24].

Należy również podkreślić zwiększenie militarnej i operacyjnej obecności USA w regionie w drugiej połowie 2025 roku poprzez patrole morskie, ćwiczenia sił specjalnych i budowanie struktur logistycznych. Przygotowania obejmowały zarówno elementy treningowe, jak i zabezpieczenie przestrzeni działania dla

[22] Redakcja, *Operacja Gideon, czyli pierwsza próba obalenia Maduro*, "Histmag.org", https://histmag.org/Operacja-Gideon-czyli-pierwsza-proba-obalenia-Maduro--28770 (dostęp: 11.02.2026 r.).

[23] U.S. Department of State, *Reward Offer Increase of Up to $50 Million for Information Leading to Arrest and/or Conviction of Nicolás Maduro*, "U.S. Department of State", https://www.state.gov/reward-offer-increase-of-up-to-50-million-for-information-leading-to-arrest-and-or-conviction-of-nicolas-maduro (dostęp: 11.02.2026 r.).

[24] M. Parraga, J. Saul, *Over 30 sanctioned ships in Venezuela at risk after US tanker seizure*, "Reuters", https://www.reuters.com/business/energy/over-30-sanctioned-ships-venezuela-risk-after-us-tanker-seizure-2025-12-11/?.com (dostęp: 11.02.2026 r.).

jednostek wywiadowczych i sił specjalnych. Ten etap był konieczny, by móc przejść od presji pośredniej do operacji bezpośredniej bez nadmiernego ryzyka dla sił interwencyjnych[25].

Koniec 2025 roku i początek stycznia 2026 roku to moment, w którym działania przygotowawcze zmaterializowały się w operacjach morskich i uderzeniach na wyizolowane cele. Nasiliły się wówczas boardingi i zatrzymania jednostek powiązanych z dostawami ropy. Działania te miały na celu dalsze zmniejszenie zasobów reżimu i jednocześnie ograniczenie możliwości ewakuacji kluczowych osób i aktywów. Równocześnie trwała intensywna koordynacja wywiadowcza, by precyzyjnie zidentyfikować lokalizacje celów i minimalizować skutki uboczne operacji[26].

Kulminacją była zaplanowana operacja kinetyczna z 3 stycznia 2026 roku, przeprowadzona przez siły specjalne i służby wywiadowcze. Akcja, która doprowadziła do zatrzymania Nicolása Maduro i jego żony oraz ich przetransportowania ich do Stanów Zjednoczonych. W następnych tygodniach po ekstrakcji Maduro rozpoczął się proces karny w USA. Przedstawiono mu zarzuty związane m.in. z przemytem narkotyków i praniem pieniędzy, a obrana linia obrony kwestionowała zarówno podstawy materii zarzutów, jak i legalność samego zatrzymania ze względu na immunitet głowy państwa[27]. Jednocześnie Waszyngton wszczął procedury zabezpieczające aktywa PDVSA i wydawał licencje operacyjne, które miały umożliwić minimalne funkcjonowanie sektora paliwowego pod kontrolą administracyjną do czasu uporządkowania sytuacji politycznej[28].

Interwencja USA niesie za sobą konsekwencje międzynarodowe. Głowa państwa ma pełny immunitet przed sądami innych państw, co podważa legalność działań USA i sugeruje erozję prawa międzynarodowego.

Podsumowanie

Interwencja militarna i przymusowe usunięcie głowy państwa mają charakter przełomowy dla dynamiki konfliktu między USA a Wenezuelą i niosą ze sobą złożone konsekwencje prawne, polityczne, ekonomiczne i społeczne. Akt ten stawia bowiem pytania o zgodność z prawem międzynarodowym, w szczególności w zakresie immunitetu głów państwa i zakazu użycia siły wobec suwerennych państw.

---

[25] I. Ali, E. Banco, S. Holland, P. Stewart, *Mock house, CIA source and Special Forces: The US operation to capture Maduro*, "Reuters", https://www.reuters.com/business/aerospace-defense/mock-house-cia-source-special-forces-us-operation-capture-maduro-2026-01-03/?.com (dostęp: 11.02.2026 r.).

[26] I. Ali, P. Stewart, *Exclusive: US seizes Venezuela-linked, Russian-flagged oil tanker after weeks-long pursuit*, "Reuters", https://www.reuters.com/business/energy/us-seizing-venezuela-linked-oil-tanker-after-weeks-long-pursuit-2026-01-07/?.com (dostęp: 11.02.2026 r.).

[27] *Vienna Convention on Diplomatic Relations*, 1961, art. 31.

[28] M. Olay, *Trump Announces U.S. Military's Capture of Maduro*, U.S. Department of War, https://www.war.gov/News/News-Stories/Article/Article/4370431/trump-announces-us-militarys-capture-of-maduro/ (dostęp: 11.02.2026 r.).

Sytuacja ta wywołuje realne reperkusje w zakresie legitymizacji działań i tworzy precedens wpływający na równowagę norm międzynarodowych. Analiza konfliktu między USA a Wenezuelą wskazuje, że kroki polityczne o charakterze delegitymizacyjnym już od dawna były wykorzystywane jako narzędzie polityki zagranicznej, teraz jednak wzmocnione zostają bezpośrednim użyciem siły, co radykalnie zmienia charakter ich stosowania.

Kolejną kwestią są skutki geopolityczne obejmujące przedefiniowanie relacji w regionie oraz przetasowania między mocarstwami. Zależność Caracas od wsparcia politycznego i materialnego ze strony partnerów takich jak Rosja, Chiny czy Kuba była jednym z czynników zwiększających koszty interwencji i komplikujących kalkulacje decydentów. Usunięcie Maduro wpłynie na równowagę wpływów, handel surowcami oraz przyszłe układy bezpieczeństwa w Ameryce Łacińskiej, ale jednocześnie może spotkać się z reakcją i próbami rekompensaty ze strony tych zewnętrznych aktorów.

Ponadto implikacje wewnętrzne dla Wenezueli są dwojakie. Krótkoterminowo interwencja może otworzyć możliwość zmiany personalnej i dostępu do aktywów, które wcześniej finansowały aparat władzy, natomiast długoterminowo jednak ryzykuje się destabilizacją instytucjonalną, pogłębieniem podziałów społecznych oraz komplikacjami w procesie odbudowy gospodarczej i humanitarnej. Dylematy dotyczące proporcjonalności środków i kosztów społecznych stają się centralne, zwłaszcza w kontekście ogromnych potrzeb humanitarnych i migracyjnych, które już wcześniej wynikały z kryzysu gospodarczego.

Wreszcie, konsekwencje dla polityki zagranicznej USA i prawa międzynarodowego skłaniają do refleksji nad instrumentarium polityki zewnętrznej. A mianowicie czy dalsza normalizacja praktyki delegitymizacji władzy połączonej z sankcjami i interwencją militarną nie będzie podkopywać długoterminowych celów stabilizacji i praworządności. Analiza doświadczeń z Wenezuelą sugeruje, że polityka powinna łączyć presję z szeroko pojmowanym planem polityczno-ekonomicznym obejmującym zabezpieczenie stabilności dostaw surowców, mechanizmu pomocy humanitarnej oraz strategie reintegracji instytucji państwowych, inaczej koszt polityczny i ludzki może przewyższyć krótkoterminowe zyski strategiczne.

Bibliografia

Aray H., Vera D., *A tale of oil production collapse*, "Resources Policy" 2024, Vol. 93.

Bull B., *Into the shadows: sanctions, rentierism, and economic informalization in Venezuela*, "European Review of Latin American and Caribbean Studies Revista Europea de Estudios Latinoamericanos y del Caribe" 2020.

Congressional Research Service, *Venezuela: Background and U.S. Relations*, "Congressional Research Service" 2022.

Galbraith J., *United States Recognizes the Opposition Government in Venezuela and Imposes Sanctions as Tensions Escalate*, "American Journal of International Law" 2019.

Iskandarov K., *Economic coercion as a means of hybrid warfare: The South Caucasus as a focal point*, "Security and Defence Quarterly" 2022.

Karl T.L., *The Paradox of Plenty: Oil Booms and Petro-States*, "University of California Press", 1997.

Monaldi F, Hernández I., La Rosa J., *The Collapse of the Venezuelan Oil Industry*, "Center for Energy Studies" 2020.

Mu X.-Z., Hu G.-W., *Analysis of Venezuela's oil-oriented economy from the perspective of entropy*, "Resources Policy" 2018.

Thoene U., *Russia in Latin America: Why support Venezuela in a crisis?*, "International Social Science Journal" 2023, Vol. 73, Issue 248.

Villa R.D., *Venezuela: political changes in the Chávez era*, "Estudios Avanzados" 2005.

Prawodawstwo

Vienna Convention on Diplomatic Relations, 1961.

Netografia

Ali I., Banco E., Holland S., Stewart P., *Mock house, CIA source and Special Forces: The US operation to capture Maduro*, "Reuters", https://www.reuters.com/business/aerospace-defense/mock-house-cia-source-special-forces-us-operation-capture-maduro-2026-01-03/?.com

Ali I., Stewart P., *Exclusive: US seizes Venezuela-linked, Russian-flagged oil tanker after weeks-long pursuit*, "Reuters", https://www.reuters.com/business/energy/us-seizing-venezuela-linked-oil-tanker-after-weeks-long-pursuit-2026-01-07/?.com

Isbell P., *Hugo Chávez and the Future of Venezuelan Oil (I): The Resurgence of Energy Nationalism (ARI)*, "Real Instituto Elcano", https://www.realinstitutoelcano.org/en/analyses/hugo-chavez-and-the-future-of-venezuelan-oil-i-the-resurgence-of-energy-nationalism-ari/?.com

Olay M., *Trump Announces U.S. Military's Capture of Maduro*, U.S. Department of War, https://www.war.gov/News/News-Stories/Article/Article/4370431/trump-announces-us-militarys-capture-of-maduro/

Parraga M., Saul J., *Over 30 sanctioned ships in Venezuela at risk after US tanker seizure*, "Reuters", https://www.reuters.com/business/energy/over-30-sanctioned-ships-venezuela-risk-after-us-tanker-seizure-2025-12-11/?.com

Parraga M., *Venezuela must pay Conoco over $8 billion - World Bank*, "Reuters", https://www.reuters.com/article/world/venezuela-must-pay-conoco-over-8-billion-world-bank-idUSKCN1QP20I/?.com

Redakcja, *Operacja Gideon, czyli pierwsza próba obalenia Maduro*, "Histmag.org", https://histmag.org/Operacja-Gideon-czyli-pierwsza-proba-obalenia-Maduro--28770

Reuters, *Chavez drives Exxon and ConocoPhillips from Venezuela*, "Reuters", https://www.reuters.com/article/business/chavez-drives-exxon-and-conocophillips-from-venezuela-idUSN26378950/?.com

Reuters, *US extends protection of Venezuela-owned Citgo from creditors*, "Reuters", https://www.reuters.com/business/energy/us-extends-protection-venezuela-owned-citgo-creditors-2026-02-02/?.com

U.S. Department of State, *Reward Offer Increase of Up to $50 Million for Information Leading to Arrest and/or Conviction of Nicolás Maduro*, "U.S. Department of State", https://www.state.gov/reward-offer-increase-of-up-to-50-million-for-information-leading-to-arrest-and-or-conviction-of-nicolas-maduro

Paweł JARGUT[1]

ZAGROŻENIA CYBERATAKÓW – ANALIZA WYBRANYCH PRZYPADKÓW

Celem niniejszego opracowania jest szczegółowa analiza współczesnych zagrożeń płynących z cyberprzestrzeni oraz identyfikacja mechanizmów leżących u podstaw skutecznych ataków teleinformatycznych na wybrane organizacje. W pracy wykorzystano metodę analityczno-porównawczą, opierając się na krytycznym przeglądzie literatury przedmiotu oraz studiach przypadków czterech znaczących incydentów: Colonial Pipeline, WannaCry, Equifax oraz Yahoo. W części teoretycznej zdefiniowano istotę cyberataków, sklasyfikowano ich rodzaje oraz omówiono motywacje i profile sprawców, wskazując na rosnącą profesjonalizację grup przestępczych. Wyniki przeprowadzonej analizy przypadków dowodzą, że najczęstszymi przyczynami paraliżu infrastruktury krytycznej oraz masowych wycieków danych są zaniedbania w podstawowej higienie cyfrowej, takie jak brak wieloskładnikowego uwierzytelniania czy zaniechanie aktualizacji systemów. Zauważono, że skutki tych incydentów wykraczają poza sferę technologiczną, generując ogromne straty finansowe, wizerunkowe oraz prawne. Główne wnioski płynące z badań podkreślają, że czynnik ludzki pozostaje najsłabszym ogniwem w łańcuchu zabezpieczeń, co czyni socjotechnikę jednym z najgroźniejszych wektorów ataku. Stwierdzono, że budowanie odporności cyfrowej organizacji wymaga holistycznego podejścia, łączącego zaawansowane systemy techniczne z ciągłą edukacją pracowników oraz sformalizowanymi procedurami reagowania na incydenty. Wskazano, iż w obliczu dynamicznie zmieniającego się krajobrazu zagrożeń, kluczowe znaczenie ma strategia obrony w głąb oraz proaktywne zarządzanie podatnościami, co pozwala na skuteczną minimalizację ryzyka w środowisku sieciowym.

Słowa kluczowe: cyberatak, bezpieczeństwo informacji, socjotechnika, infrastruktura krytyczna, wyciek danych, zarządzanie ryzykiem, higiena cyfrowa.

Teoretyczne aspekty cyberbezpieczeństwa i zagrożeń w sieci

Na wstępie rozważań nad zagadnieniem zagrożeń w sieci warto zdefiniować pojęcie cyberataku. W literaturze przedmiotu wskazano na wiele ujęć tego terminu, jednak najczęściej cyberatak uznawano za celowe i wrogie działanie, którego celem było zakłócenie, uszkodzenie lub uzyskanie nieuprawnionego dostępu do systemów informatycznych[2]. Zauważono również, że kluczową kwestią w rozumieniu istoty incydentów sieciowych było naruszenie podstawowych

[1] Paweł Jargut, student Politechniki Rzeszowskiej im. Ignacego Łukasiewicza, Koło Naukowe Polityki Bezpieczeństwa Państwa. ORCID: 0009-0003-2447-0488.

[2] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, s. 12.

atrybutów bezpieczeństwa informacji, czyli poufności, integralności oraz dostępności[3].

Analizie poddano istotę zjawisk zachodzących w środowisku cyfrowym, w którym zidentyfikowano znaczący wzrost aktywności przestępczej. Ustalono, że ataki wymierzone były w najsłabsze ogniwa systemów teleinformatycznych, którymi nierzadko okazywali się sami użytkownicy[4]. Wskazano, że sprawcy wykorzystywali zjawisko inżynierii społecznej oraz zaawansowane techniki, aby przełamać zabezpieczenia i uzyskać dostęp do poufnych danych[5].

W toku analizy raportów dotyczących bezpieczeństwa wyodrębniono oraz opisano główne rodzaje zagrożeń. Zestawienie najpopularniejszych typów cyberataków przedstawiono w następujący sposób[6]:

1. Złośliwe oprogramowanie *(malware*). Zidentyfikowano je jako programy, których celem było uszkodzenie sprzętu, kradzież danych lub przejęcie kontroli nad systemem. Do tej grupy zaliczono między innymi wirusy, trojany oraz oprogramowanie szpiegujące[7].
2. Oprogramowanie wymuszające okup (*ransomware*). Uznane za jeden z najbardziej niszczycielskich rodzajów ataków w cyberprzestrzeni. Stwierdzono, że atak ten polegał na szyfrowaniu danych, a następnie żądaniu okupu za przywrócenie do nich dostępu[8].
3. Ataki socjotechniczne oraz *phishing*. Zauważono, że w tego typu operacjach przestępcy manipulowali użytkownikami, podszywając się pod zaufane podmioty w celu wyłudzenia informacji finansowych lub haseł[9].
4. Ataki typu DoS i DDoS (*Denial of Service*). Ustalono, że polegały one na generowaniu sztucznego ruchu sieciowego, który przeciążał łącza firmowe i całkowicie blokował użytkownikom dostęp do usług[10].
5. Kradzież tożsamości oraz manipulacja bazami danych. Zaobserwowano, że działania te zmierzały bezpośrednio do nielegalnego przejęcia danych w celu ich skopiowania (np. poprzez techniki SQL Injection) lub zmiany[11].

---

[3] D. Skoczylas, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, „Prawo w Działaniu" 2023, nr 53, s. 102.

[4] *Cyberbezpieczeństwo teoretycznie i empirycznie w naukach o bezpieczeństwie*, red. A. Janczewski, Morskie Centrum Cyberbezpieczeństwa, Gdynia 2022, s. 45.

[5] *Rodzaje i cechy charakterystyczne cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa*, „Zeszyty Naukowe WSB" 2024, Poznań, s. 55.

[6] P. Smerdel, *Informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni*, BIP Starostwo Powiatowe w Kwidzynie, https://bip.powiatkwidzynski.pl/artykul/informacje-pozwalajace-na-zrozumienie-zagrozen-wystepujacych-w-cyberprzestrzeni-oraz-porady-ja (dostęp: 18.04.2026 r.).

[7] M. Lakomy, *Cyberprzestrzeń...*, dz. cyt., s. 15.

[8] *Raport roczny z działalności CERT Polska w 2025 roku*, NASK, Warszawa 2026, s. 15.

[9] *Cyberbezpieczeństwo teoretyczne...*, dz. cyt., s. 48.

[10] P. Smerdel, *Informacje pozwalające...*, dz. cyt.

[11] *Rodzaje i cechy charakterystyczne...*, dz. cyt., s. 58.

Podsumowując, warto zwrócić uwagę na rosnące znaczenie obrony przed zidentyfikowanymi zagrożeniami. Znajomość najbardziej typowych form cyberataków oraz metod ochrony określono jako podstawową kompetencję współczesnych pracowników i instytucji[12].

Motywacje oraz profile współczesnych cyberprzestępców

W ramach niniejszego podrozdziału warto pochylić się nad charakterystyką podmiotów odpowiedzialnych za realizację ataków w cyberprzestrzeni oraz przeanalizować czynniki skłaniające ich do podejmowania działań o charakterze przestępczym. Ewolucja technologii informacyjnych wpłynęła na znaczącą zmianę profilu sprawcy – od amatorów poszukujących jedynie uznania w środowisku, po wysoko wyspecjalizowane grupy działające na zlecenie państw lub międzynarodowych organizacji przestępczych[13].

Dokonano klasyfikacji głównych motywacji, którymi kierowali się sprawcy incydentów sieciowych. W literaturze przedmiotu wyodrębniono następujące grupy pobudek[14]:

1. zysk finansowy – uznano go za najczęstszy powód podejmowania ataków. Działania te obejmowały kradzież danych bankowych, wymuszanie okupów przy użyciu oprogramowania typu ransomware czy handel poufnymi informacjami na czarnym rynku[15],
2. pobudki ideologiczne i polityczne – zidentyfikowano je jako fundament działań podejmowanych przez tzw. haktywistów. Celem było wówczas wyrażenie sprzeciwu wobec decyzji politycznych, nagłośnienie problemów społecznych lub uderzenie w wizerunek konkretnej instytucji[16],
3. szpiegostwo przemysłowe i państwowe – wskazano, że ataki te ukierunkowane były na zdobycie przewagi technologicznej, kradzież własności intelektualnej lub pozyskanie tajnych informacji o charakterze strategicznym dla bezpieczeństwa państwa[17],
4. pobudki osobiste oraz chęć sprawdzenia własnych umiejętności – zauważono, że część sprawców traktowała ataki jako wyzwanie techniczne lub sposób na zdobycie autorytetu w podziemiu hakerskim[18].

---

[12] *Raport roczny z działalności CERT Polska...*, dz. cyt., s. 22.
[13] W. Filipkowski, *Zwalczanie cyberprzestępczości*, Wydawnictwo Wolters Kluwer, Warszawa 2012, s. 42.
[14] A. Adamski, *Przestępczość w świecie cyfrowym*, Wydawnictwo C.H. Beck, Warszawa 2017, s. 88.
[15] *Krajobraz zagrożeń w cyberprzestrzeni. Raport roczny ENISA*, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa,https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (dostęp: 18.04.2026 r.).
[16] K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski*, Wydawnictwo Difin, Warszawa 2011, s. 115.
[17] J. Kosiński, *Paradygmaty cyberprzestrzeni*, Wydawnictwo Difin, Warszawa 2015, s. 134.
[18] W. Filipkowski, *Zwalczanie cyberprzestępczości...*, dz. cyt., s. 45.

W toku dalszych badań poddano analizie profile osób i grup operujących w środowisku cyfrowym. Na podstawie zebranych danych można opracować typologię współczesnych cyberprzestępców[19]:

1. Amatorzy (tzw. *script kiddies*). Określono ich jako osoby o stosunkowo niskich kompetencjach technicznych, które korzystały z gotowych, dostępnych w sieci narzędzi i skryptów do przeprowadzania nieskomplikowanych ataków.
2. Cyberprzestępcy zawodowi i grupy zorganizowane. Scharakteryzowano ich jako podmioty działające stricte dla zysku, posiadające strukturę hierarchiczną i dysponujące znacznymi środkami na rozwój złośliwego oprogramowania.
3. Grupy typu Advanced Persistent Threat (APT). Ustalono, że były to zespoły wysokiej klasy specjalistów, często finansowane i wspierane przez rządy państw, realizujące długofalowe operacje wymierzone w infrastrukturę krytyczną innych krajów[20].
4. Pracownicy i osoby z wewnątrz organizacji (insiderzy). Zwrócono uwagę na szczególne zagrożenie wynikające z działań osób posiadających uprawniony dostęp do systemów, które wykorzystywały swoją pozycję do sabotażu lub kradzieży danych[21].

W tym miejscu należy podkreślić, że zrozumienie profilu sprawcy oraz jego motywacji stanowi kluczowy element budowania skutecznych strategii obronnych w każdej nowoczesnej organizacji[22].

Wpływ incydentów sieciowych na funkcjonowanie organizacji

Warto przeanalizować wpływ incydentów sieciowych na funkcjonowanie przedsiębiorstw oraz instytucji państwowych. W literaturze przedmiotu oraz najnowszych raportach branżowych wskazuje się, że cyberataki dawno przestały być wyłącznie problemem natury technologicznej, stając się jednym z najpoważniejszych ryzyk biznesowych[23].

Podkreśla się, że skutki przełamania zabezpieczeń mają wymiar wielopłaszczyznowy i często prowadzą do długotrwałego paraliżu działalności operacyjnej organizacji[24].

---

[19] *Profil cyberprzestępcy i metodyka ataków*, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/cyberbezpieczenstwo (dostęp: 18.04.2026 r.).

[20] A. Adamski, *Przestępczość w świecie...*, dz. cyt., s. 92.

[21] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, Ministerstwo Cyfryzacji, Warszawa 2024, s. 31.

[22] J. Kosiński, *Paradygmaty...*, dz. cyt., s. 138.

[23] K. Pasławski, *3/4 incydentów cyberbezpieczeństwa wynika z niezarządzanych zasobów*, CRN Polska, https://crn.pl/aktualnosci/3-4-incydentow-cyberbezpieczenstwa-wynika-z-niezarzadzanych-zasobow-cyberataki/ (dostęp: 18.04.2026 r.).

[24] *Cyberbezpieczeństwo teoretycznie…,* dz. cyt., s. 89.

Na podstawie analizy globalnych danych wyodrębnia się cztery główne obszary, w których współczesne organizacje ponoszą największe straty w wyniku cyberataków:

1. Skutki finansowe – zauważa się, że koszty związane z cyberprzestępczością rosną w bezprecedensowym tempie. Szacuje się, że globalne koszty incydentów sieciowych mogą osiągnąć poziom 10,5 biliona dolarów rocznie w 2025 roku[25]. Wskazuje się, że straty te obejmują zarówno koszty bezpośrednie, takie jak wypłata okupów, wynajęcie zewnętrznych ekspertów informatycznych czy odbudowa infrastruktury, jak i utracone przychody wynikające z przymusowych przestojów[26].
2. Zakłócenia ciągłości działania (operacyjne) – stwierdza się, że ataki z wykorzystaniem złośliwego oprogramowania (np. *ransomware*) oraz ataki wolumetryczne (DDoS) bezpośrednio wymuszają na organizacjach wstrzymanie działania krytycznych systemów[27]. Zwraca się uwagę, że przestoje te uniemożliwiają obsługę klientów i realizację zamówień, a proces przywracania usług z kopii zapasowych zajmuje nierzadko od kilku dni do nawet kilku tygodni[28].
3. Utrata wizerunku i zaufania klientów – uznaje się, że szkody reputacyjne są często najtrudniejszym do przezwyciężenia skutkiem incydentów bezpieczeństwa. Obserwuje się, że wyciek poufnych danych klientów prowadzi do natychmiastowej utraty zaufania, co bezpośrednio przekłada się na masowy odpływ konsumentów, spadek cen akcji oraz ogromne trudności w pozyskiwaniu nowych partnerów biznesowych[29].
4. Konsekwencje prawno-regulacyjne – przypomina się, że podmioty gospodarcze są zobowiązane do ścisłej ochrony gromadzonych danych na mocy przepisów, takich jak unijne rozporządzenie RODO. Zaznacza się, że poważne naruszenia bezpieczeństwa i kradzież danych skutkują nałożeniem wielomilionowych kar administracyjnych (sięgających nawet 20 milionów euro lub 4% rocznego światowego obrotu przedsiębiorstwa), a także narażają organizację na zbiorowe pozwy cywilne poszkodowanych użytkowników[30].

---

[25] Z. Łochowska, *Statystyki cyberbezpieczeństwa - najnowsze dane o cyberatakach 2025*, Exorigo-Upos, https://www.exorigo-upos.pl/blog/statystyki-cyberbezpieczenstwa-dane-z-2025-roku/ (dostęp: 18.04.2026 r.).

[26] *Globalny koszt cyberataków w 2026 r.*, Blog ExpressVPN, https://www.expressvpn.com/pl/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/ (dostęp: 18.04.2026 r.).

[27] *The Impact of Cybercrime on Business*, Ponemon Institute, 2024, s. 2.

[28] *Co to jest cyberatak?*, Microsoft Security, https://www.microsoft.com/pl-pl/security/business/security-101/what-is-a-cyberattack (dostęp: 18.04.2026 r.).

[29] *Cyberprzestępczość 2025: Jakie branże są najbardziej narażone na ataki hakerskie?*, Bitdefender, https://bitdefender.pl/cyberprzestepczosc-2025-jakie-branze-sa-najbardziej-narazone-na-ataki-hakerskie/ (dostęp: 18.04.2026 r.).

[30] Z. Łochowska, *Statystyki cyberbezpieczeństwa – najnowsze dane...*, dz. cyt.

Analizując to zestawienie, widać, że wpływ cyberataków na organizacje ma charakter destrukcyjny i długoterminowy. Argumentuje się, że brak proaktywnego zarządzania ryzykiem informatycznym stanowi obecnie bezpośrednie zagrożenie nie tylko dla rynkowej pozycji przedsiębiorstwa, ale w skrajnych przypadkach dla jego dalszego przetrwania[31].

Analiza wybranych przypadków cyberataków

Przechodząc do studium przypadków warto poddać analizie jeden z najbardziej przełomowych ataków na infrastrukturę krytyczną w historii Stanów Zjednoczonych, czyli incydent wymierzony w sieć rurociągów Colonial Pipeline w maju 2021 roku[32]. Wskazuje się, że atak ten obnaża drastyczne luki w zabezpieczeniach systemów przemysłowych, a jego skutki wykraczają daleko poza samą sferę cyfrową, uderzając bezpośrednio w stabilność gospodarczą i logistyczną państwa[33].

Analizując wektor ataku, z którego korzystają napastnicy ustalono, że za incydent odpowiada wschodnioeuropejska grupa cyberprzestępcza DarkSide, operująca w modelu biznesowym określanym jako oprogramowanie wymuszające okup w ramach usługi (ang. *Ransomware-as-a-Service*, RaaS)[34]. Zwraca się szczególną uwagę na fakt, że do przełamania zabezpieczeń firmy nie wykorzystuje się skomplikowanych podatności oprogramowania (tzw. zero-day), lecz skompromitowane. Nieaktywne konto wirtualnej sieci prywatnej (VPN) należące do jednego z pracowników[35]. Zauważa się, że hasło do tego konta zostało wcześniej ujawnione w sieci darknet, a dostęp do firmowego VPN nie był dodatkowo chroniony uwierzytelnianiem wieloskładnikowym (MFA), co pozwala hakerom na swobodne przeniknięcie do systemów korporacyjnych przedsiębiorstwa[36].

W toku badania przebiegu incydentu wyodrębnia się następujące, kluczowe fazy ataku oraz jego rynkowe konsekwencje:

1. Kradzież danych przed szyfrowaniem – obserwuje się, że napastnicy stosują taktykę podwójnego wymuszenia. Przed uruchomieniem złośliwego oprogramowania blokującego urządzenia, sprawcy kradną z serwerów około 100 gigabajtów wrażliwych danych, grożąc ich upublicznieniem w razie odmowy zapłaty okupu[37].

---

[31] K. Pasławski, *3/4 incydentów cyberbezpieczeństwa...*, dz. cyt.

[32] *USA. Atak hakerski na sieć rurociągów Colonial Pipeline*, TVN24, https://tvn24.pl/swiat/usa-atak-hakerski-na-siec-rurociagow-colonial-pipeline-5090075 (dostęp: 19.04.2026 r.).

[33] *How a secure MFA would have avoided the Colonial cyberattack*, WatchGuard, https://www.watchguard.com/fr/wgrd-news/blog/how-secure-mfa-would-have-avoided-colonial-cyberattack (dostęp: 19.04.2026 r.).

[34] *USA. Atak hakerski na sieć rurociągów…,* dz. cyt.

[35] *How a secure MFA would…,* dz. cyt.

[36] Tamże.

[37] *Colonial Pipeline ransomware attack*, Wikipedia, https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack (dostęp: 19.04.2026 r.).

2. Przerwanie ciągłości działania infrastruktury przemysłowej – wskazuje się, że chociaż atak ransomware dotyka bezpośrednio systemów informatycznych (IT) odpowiedzialnych za księgowość i zarządzanie, to z obawy przed przeniknięciem złośliwego kodu do technologii operacyjnych (OT), zarząd Colonial Pipeline podejmuje bezprecedensową decyzję o zapobiegawczym wyłączeniu całego rurociągu o długości 5500 mil[38].
3. Paraliż społeczno-gospodarczy – odnotowuje się, że wstrzymanie przesyłu paliwa wywołuje natychmiastowe niedobory benzyny, diesla i paliwa lotniczego na wschodnim wybrzeżu USA[39]. Stwierdza się, że zjawisko masowego wykupywania paliwa przez zaniepokojonych obywateli (tzw. *panic buying*) prowadzi do całkowitego opróżnienia zbiorników na stacjach, a kryzysowa sytuacja zmusza rząd amerykański do ogłoszenia regionalnego stanu wyjątkowego w kilkunastu stanach[40].
4. Kwestia zapłaty okupu – zauważa się, że pod ogromnym naciskiem opinii publicznej i widmem przedłużającego się paraliżu transportu, firma podejmuje szybką decyzję o zapłaceniu grupie hakerskiej żądanej kwoty w bitcoinach (stanowiącej wówczas równowartość ok. 4,4 miliona dolarów) w zamian za narzędzie deszyfrujące i wznowienie operacji[41].

Podsumowując powyższy przypadek można wyciągnąć wniosek, że incydent ten stanowi wyraźny punkt zwrotny w polityce ochrony infrastruktury krytycznej. Dowodzi się, że nawet najbardziej kosztowne systemy obronne zawodzą, jeśli nie przestrzega się absolutnych podstaw rygoru cyfrowego. Przypadek Colonial Pipeline pokazuje, że zlekceważenie jednego loginu bez włączonej autoryzacji dwuetapowej może zatrzymać strategiczne dostawy surowców dla milionów obywateli[42].

Atak ransomware znany jako WannaCry stanowi jeden z najbardziej znaczących incydentów cyberbezpieczeństwa w historii współczesnej. Został on przeprowadzony w maju 2017 roku i w krótkim czasie objął zasięgiem ponad 150 państw, infekując setki tysięcy komputerów na całym świecie. Atak ten ujawnił skalę zagrożeń wynikających z podatności systemów informatycznych oraz braku odpowiednich zabezpieczeń w wielu instytucjach publicznych |i prywatnych[43].

WannaCry należał do kategorii oprogramowania typu ransomware, którego głównym celem było zaszyfrowanie danych użytkownika i wymuszenie okupu za

---

[38] Tamże.

[39] *Infrastruktura jest łatwym celem cyberataków*, Obserwator Finansowy, https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/infrastruktura-jest-latwym-celem-cyberatakow/ (dostęp: 19.04.2026 r.).

[40] *Colonial Pipeline ransomware…,* dz. cyt.

[41] *Prezes Colonial Pipeline potwierdza: zapłaciliśmy okup hakerom*, CyberDefence24, https://cyberdefence24.pl/biznes-i-finanse/prezes-colonial-pipeline-potwierdza-zaplacilismy-okup-hakerom (dostęp: 19.04.2026 r.).

[42] *How a secure MFA…,* dz. cyt.

[43] A. Greenberg, *This Is How WannaCry Spread – and Why It Could Happen Again*, Wired, 2017, https://www.wired.com/story/wannacry-ransomware-worm/ (dostęp: 19.04.2026 r.).

ich odblokowanie[44]. Wykorzystywał on lukę w systemie operacyjnym Microsoft Windows, znaną jako EternalBlue, która umożliwiała zdalne wykonywanie kodu bez wiedzy użytkownika. Luka ta została wcześniej zidentyfikowana przez National Security Agency, a następnie ujawniona przez grupę hakerską Shadow Brokers, co przyczyniło się do jej wykorzystania w szeroko zakrojonym ataku[45].

Mechanizm działania WannaCry polegał na automatycznym rozprzestrzenianiu się w sieci poprzez wykorzystanie podatnych urządzeń. Po zainfekowaniu komputera następowało szyfrowanie plików, a użytkownik otrzymywał komunikat z żądaniem zapłaty okupu w kryptowalucie Bitcoin. Charakterystyczną cechą tego ataku była jego zdolność do samodzielnego rozprzestrzeniania się (tzw. worm), co znacząco zwiększyło skalę infekcji[46].

Szczególnie dotkliwe skutki ataku odnotowano w sektorze publicznym, zwłaszcza w systemie opieki zdrowotnej w Wielkiej Brytanii. W wyniku infekcji sparaliżowana została działalność wielu placówek należących do National Health Service, co doprowadziło do odwołania zabiegów oraz utrudnienia dostępu do opieki medycznej[47]. Straty odnotowały również przedsiębiorstwa oraz instytucje na całym świecie, co potwierdziło globalny charakter zagrożenia[48].

W kontekście odpowiedzialności za atak, wiele analiz wskazuje na powiązania z grupami hakerskimi działającymi na rzecz Korei Północnej, w szczególności z grupą Lazarus[49]. Jednak ze względu na specyfikę cyberprzestrzeni jednoznaczne przypisanie odpowiedzialności pozostaje utrudnione.

Analiza ataku WannaCry prowadzi do wniosku, że jednym z kluczowych czynników umożliwiających jego sukces był brak aktualizacji systemów operacyjnych oraz niewystarczający poziom zabezpieczeń w wielu organizacjach[50]. Wydarzenie to uwidoczniło konieczność systematycznego zarządzania bezpieczeństwem informatycznym oraz szybkiego reagowania na pojawiające się podatności.

Jeden z najpoważniejszych incydentów naruszenia bezpieczeństwa danych w historii sektora finansowego, który dotyka amerykańską agencję sprawozdawczości kredytowej Equifax ma miejsce w 2017 roku[51]. Casus ten stanowił istotne studium zjawiska zaniedbań w obszarze zarządzania podatnościami systemowymi[52].

---

[44] K. Scaife i in., *Cryptolock (and Drop It): Stopping Ransomware Attacks on User Data*, IEEE, 2016.
[45] M. Suiche, *WannaCry: A Technical Analysis*, Comae Technologies, 2017.
[46] A. Greenberg, *This Is How WannaCry Spread…,* dz. cyt.
[47] European Union Agency for Cybersecurity (ENISA), *WannaCry Ransomware Outburst*, 2017.
[48] A. Greenberg, *This Is How WannaCry Spread…*, dz. cyt.
[49] European Union Agency for Cybersecurity (ENISA), *WannaCry…, dz. cyt.*
[50] M. Suiche, *WannaCry: A Technical Analysis*, Comae Technologies, dz. cyt.
[51] Redakcja Niebezpiecznik, *Ogromny wyciek z Equifax. 143 miliony Amerykanów straciło dane*, Niebezpiecznik.pl, https://niebezpiecznik.pl/post/ogromny-wyciek-z-equifax/ (dostęp: 19.04.2026 r.).
[52] K. Branecki, *Wyciek danych z Equifax – analiza anatomii ataku*, Sekurak, https://sekurak.pl/wyciek-danych-z-equifax-analiza/ (dostęp: 19.04.2026 r.).

Analizuje się bezpośredni wektor ataku, którym okazuje się znana luka w otwartym oprogramowaniu serwerowym Apache Struts. Ustalono, że choć producent udostępnia stosowną łatkę bezpieczeństwa na kilka miesięcy przed atakiem, organizacja nie wdraża jej w swoich systemach z powodu błędów w wewnętrznych procesach administracyjnych. Zauważono, że to właśnie brak prostej aktualizacji pozwala napastnikom na uzyskanie nieautoryzowanego dostępu do sieci korporacyjnej, w której przebywają oni niezauważeni przez ponad dwa miesiące[53].

W toku badania przebiegu incydentu stwierdza się, że hakerzy dokonują eksfiltracji wrażliwych danych osobowych należących do około 147 milionów konsumentów. Odnotowuje się, że skradzione zasoby obejmują między innymi numery ubezpieczenia społecznego (SSN), daty urodzenia oraz adresy zamieszkania, co naraża poszkodowanych na długofalowe ryzyko kradzieży tożsamości. Zwraca się uwagę, że sukces operacji przestępczej wynika nie tylko z braku aktualizacji, ale również z poważnych błędów w architekturze sieci, takich jak brak segmentacji oraz wygaśnięcie certyfikatów bezpieczeństwa w systemach monitorujących ruch sieciowy[54].

Podsumowując skutki finansowe i wizerunkowe, wskazuje się, że firma zostaje zmuszona do zapłaty ponad 700 milionów dolarów w ramach ugód i odszkodowań. Dowodzi się, że kryzys ten doprowadza do dymisji kluczowych osób w kierownictwie oraz trwałej utraty zaufania rynkowego do instytucji. Przypadek Equifax interpretuje się zatem jako ostrzeżenie przed bagatelizowaniem rutynowych procedur bezpieczeństwa w organizacjach przetwarzających dane na masową skalę[55].

Analizując różne cyberataki warto przytoczyć serię naruszeń bezpieczeństwa danych w firmie Yahoo, ze szczególnym uwzględnieniem incydentów z roku 2013 oraz roku 2014. Wskazuje się, że pod względem liczby poszkodowanych użytkowników, ataki te stanowią jeden z największych znanych wycieków danych w historii globalnej sieci, obejmując łącznie wszystkie trzy miliardy kont zarejestrowanych ówcześnie w serwisie[56].

Analizuje się sposób działania sprawców, wśród których organy śledcze zidentyfikowały między innymi wysoce zorganizowane grupy przestępcze. Ustalono, że początkowym wektorem ataku w 2014 roku jest spersonalizowana kampania *phishingowa* (tzw. *spear-phishing*) wycelowana w pracowników firmy, która umożliwia napastnikom dostęp do wewnętrznej sieci korporacyjnej.

---

[53] P. Kijewski, *Zarządzanie podatnościami na przykładzie ataku na firmę Equifax*, „IT Professional" 2019, nr 11, s. 34.

[54] *Report to Congressional Requesters. Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, U.S. Government Accountability Office (GAO), Washington 2018, s. 12-14.

[55] P. Kijewski, *Zarządzanie podatnościami…,* dz. cyt.

[56] P. Konieczny, *Wszystkie 3 miliardy kont Yahoo zostało zhakowanych*, Niebezpiecznik, https://niebezpiecznik.pl/post/wszystkie-3-miliardy-kont-yahoo-zostalo-zhakowanych/ (dostęp: 20.04. 2026 r.).

Zauważa się, że po udanym włamaniu cyberprzestępcy uzyskują dostęp do bazy danych użytkowników oraz zaawansowanych narzędzi do zarządzania kontami. Ponadto stwierdza się, że hakerzy skutecznie wykorzystują technikę fałszowania ciasteczek sesyjnych (ang. *forged cookies*), co pozwala im na logowanie się do profili ofiar bez konieczności podawania jakichkolwiek haseł[57].

W toku badania przebiegu incydentu odnotowuje się kradzież ogromnych ilości wrażliwych danych, w tym imion i nazwisk, adresów e-mail, dat urodzenia, numerów telefonów oraz, co najbardziej krytyczne, niezaszyfrowanych pytań i odpowiedzi pomocniczych służących do odzyskiwania dostępu. Zwraca się szczególną uwagę na fakt, że organizacja przez kilka lat ukrywa informację o wycieku przed opinią publiczną. Podkreśla się, że to zatajenie uniemożliwia użytkownikom podjęcie niezbędnych kroków ochronnych i znacząco zwiększa ryzyko wtórnych ataków na inne usługi sieciowe, w których ofiary powielają te same dane logowania[58].

Reasumując skutki finansowe i wizerunkowe incydentu, wskazuje się, że rażące opóźnienie w ujawnieniu włamania doprowadza do nałożenia na firmę wielomilionowych kar przez amerykańską Komisję Papierów Wartościowych i Giełd (SEC) za wprowadzanie inwestorów w błąd. Dowodzi się również, że ujawnienie prawdy o wycieku ma bezpośredni, negatywny wpływ na wycenę rynkową przedsiębiorstwa. Zauważa się, że w wyniku skandalu firma Yahoo zostaje zmuszona do obniżenia ceny sprzedaży swoich aktywów internetowych korporacji Verizon o 350 milionów dolarów. Przypadek ten interpretuje się zatem jako wyraźny dowód na to, że brak przejrzystości oraz niewłaściwe zarządzanie komunikacją kryzysową po incydencie generują straty finansowe, które znacznie przewyższają bezpośrednie koszty operacyjne samego ataku[59].

Zarządzanie ryzykiem i prewencja w obliczu zagrożeń cybernetycznych

Po przedstawieniu studium przypadków w poprzednim podrozdziale warto zwrócić uwagę na kluczowe strategie oraz narzędzia wykorzystywane w procesie minimalizowania ryzyka wystąpienia incydentów teleinformatycznych. Wskazuje się, że w obliczu stale ewoluujących zagrożeń, nowoczesne organizacje nie mogą opierać się wyłącznie na pojedynczych zabezpieczeniach perymetrowych. Podkreśla się konieczność stosowania podejścia warstwowego, znanego powszechnie jako obrona w głąb (ang. *defense in depth*), które zakłada ścisłą integrację

[57] Redakcja Zaufana Trzecia Strona, *Jak doszło do włamania do Yahoo i kradzieży danych pół miliarda kont*, https://zaufanatrzeciastrona.pl/post/jak-doszlo-do-wlamania-do-yahoo-i-kradziezy-danych-pol-miliarda-kont/ (dostęp: 20.04.2026 r.).

[58] Tamże.

[59] K. Branecki, *Analiza wektorów ataku i wycieków danych z Yahoo*, Sekurak, https://sekurak.pl/analiza-wyciekow-z-yahoo/ (dostęp: 20.04.2026 r.).

zróżnicowanych mechanizmów technicznych, organizacyjnych oraz proceduralnych na wielu poziomach infrastruktury sieciowej[60].

W obszarze prewencji szczególną uwagę zwraca się na fundamentalne zasady higieny cyfrowej, których zaniedbanie często prowadzi do katastrofalnych skutków. Wskazuje się na absolutną konieczność rygorystycznego zarządzania podatnościami oraz regularnego aktualizowania oprogramowania systemowego i aplikacyjnego w celu eliminacji znanych luk bezpieczeństwa. Równie istotnym elementem, na który kładzie się silny nacisk, jest wdrożenie wieloskładnikowego uwierzytelniania (MFA) dla wszystkich kont dostępowych, a w szczególności tych posiadających uprawnienia administracyjne oraz wykorzystywanych do połączeń zdalnych. Dodatkowo zauważa się, że skuteczne zapobieganie wymaga implementacji zaawansowanych systemów bezpieczeństwa, takich jak zapory sieciowe nowej generacji, systemy wykrywania i zapobiegania włamaniom (IDS/IPS) oraz oprogramowanie klasy EDR (ang. *Endpoint Detection and Response*), które w czasie rzeczywistym monitoruje zachowanie punktów końcowych i automatycznie blokuje podejrzane procesy[61].

Następnie poddaje się analizie kwestię reagowania na incydenty, wychodząc z założenia, że żaden system zabezpieczeń nie gwarantuje stuprocentowej odporności na przełamanie. Z tego względu podkreśla się kluczową rolę sformalizowanych planów reagowania na incydenty (ang. *Incident Response Plan*). Zauważa się, że skuteczne zarządzanie sytuacją kryzysową po wykryciu ataku wymaga natychmiastowej izolacji zainfekowanych segmentów sieci w celu powstrzymania rozprzestrzeniania się złośliwego kodu, a w kolejnym kroku trwałego usunięcia zagrożenia i przywrócenia systemów do działania na podstawie bezpiecznych kopii zapasowych. Dowodzi się ostatecznie, że niezwykle ważnym etapem zamykającym proces reagowania jest faza wnikliwej analizy po incydencie. To właśnie w tym czasie wyciąga się odpowiednie wnioski, modyfikuje istniejące procedury oraz łata wykryte słabości w architekturze zabezpieczeń, aby zminimalizować prawdopodobieństwo powtórzenia się podobnego scenariusza w przyszłości[62].

Rola edukacji i czynnika ludzkiego w budowaniu odporności cyfrowej

Warto również się skupić na kompetencji użytkowników oraz ich wpływ na ogólny poziom bezpieczeństwa systemów informacyjnych. W literaturze przedmiotu oraz raportach z incydentów powszechnie wskazuje się, że to właśnie człowiek, a nie technologia, stanowi najsłabsze ogniwo w łańcuchu zabezpieczeń

[60] P. Piotrowski, *Obrona w głąb jako fundament bezpieczeństwa IT*, Securitum, https://securitum.pl/obrona-w-glab-jako-fundament-bezpieczenstwa/ (dostęp: 20.04.2026 r.).

[61] M. Serafin, *Reagowanie na incydenty bezpieczeństwa sieci*, „IT Professional" 2022, nr 5, s. 42-45.

[62] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2017, s. 112.

każdej organizacji. Zauważa się, że nawet najbardziej zaawansowane rozwiązania techniczne, takie jak systemy szyfrujące czy zapory sieciowe, okazują się bezużyteczne w sytuacji, gdy nieświadomy użytkownik ulega manipulacji i samodzielnie udostępnia dane logowania przestępcom. Podkreśla się zatem, że budowanie odporności cyfrowej musi opierać się na równoległym rozwoju infrastruktury oraz świadomości kadry pracowniczej[63].

Analizie poddaje się mechanizmy socjotechniczne, które stanowią główną metodę wykorzystywania ludzkich słabości, takich jak pośpiech, chęć niesienia pomocy czy lęk przed konsekwencjami służbowymi. Stwierdza się, że najskuteczniejszą metodą przeciwdziałania tego typu zagrożeniom są regularne i wielopoziomowe programy szkoleniowe typu *Security Awareness.* Wskazuje się, że edukacja ta nie powinna ograniczać się jedynie do przekazywania teoretycznej wiedzy, lecz musi obejmować praktyczne warsztaty oraz kontrolowane testy socjotechniczne, na przykład w formie symulowanych kampanii phishingowych. Zauważa się, że dzięki takim działaniom pracownicy nabywają umiejętność krytycznej oceny otrzymywanych wiadomości i uczą się prawidłowych reakcji na nietypowe żądania systemowe[64].

W toku rozważań nad czynnikiem ludzkim zwraca się również uwagę na konieczność kształtowania trwałej kultury bezpieczeństwa wewnątrz organizacji. Uznaje się, że odporność cyfrowa wzrasta w momencie, gdy każdy członek zespołu, niezależnie od zajmowanego stanowiska, czuje się współodpowiedzialny za ochronę zasobów informacyjnych firmy. Zaznacza się, że proces ten wymaga jasnej komunikacji zasad bezpieczeństwa oraz stworzenia środowiska, w którym zgłaszanie potencjalnych incydentów lub popełnionych błędów jest premiowane, a nie karane. Argumentuje się ostatecznie, że edukacja w obszarze cyberbezpieczeństwa jest procesem ciągłym, który musi nadążać za dynamicznie zmieniającym się krajobrazem zagrożeń w przestrzeni wirtualnej[65].

Bibliografia

Adamski A., *Przestępczość w świecie cyfrowym*, Wydawnictwo C.H. Beck, Warszawa 2017.

Cyberbezpieczeństwo teoretycznie i empirycznie w naukach o bezpieczeństwie, red. A. Janczewski, Morskie Centrum Cyberbezpieczeństwa, Gdynia 2022.

Filipkowski W., *Zwalczanie cyberprzestępczości*, Wydawnictwo Wolters Kluwer, Warszawa 2012.

Fuksiewicz M., *Rodzaje i cechy charakterystyczne cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa*, „Zeszyty Naukowe WSB" 2024, nr 102(3).

Kijewski P., *Zarządzanie podatnościami na przykładzie ataku na firmę Equifax*, IT Professional, 2019, nr 11.

Kosiński J., *Paradygmaty cyberprzestrzeni*, Wydawnictwo Difin, Warszawa 2015.

[63] J. Kosiński, *Paradygmaty cyberprzestrzeni…*, dz. cyt., s. 92.
[64] *Raport roczny z działalności CERT Polska w 2025 roku*, NASK, Warszawa 2026, s. 45.
[65] J. Kosiński, *Paradygmaty cyberprzestrzeni…*, dz. cyt., s. 92.

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.

Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2017.

Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski*, Wydawnictwo Difin, Warszawa 2011.

Serafin M., *Człowiek jako najsłabsze ogniwo – jak szkolić pracowników w dobie socjotechniki*, „IT Professional" 2023, nr 2.

Serafin M., *Reagowanie na incydenty bezpieczeństwa sieci*, „Magazyn IT Professional" 2022, nr 5.

Serafin M., *SolarWinds: anatomia ataku, który wstrząsnął światem IT*, „Magazyn IT Professional" 2021, nr 3.

Skoczylas D., *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, „Prawo w Działaniu" 2023 nr 53.

The Impact of Cybercrime on Business, Ponemon Institute, 2024.

Netografia

3/4 incydentów cyberbezpieczeństwa wynika z niezarządzanych zasobów, CRN Polska, https://crn.pl/aktualnosci/3-4-incydentow-cyberbezpieczenstwa-wynika-z-niezarzadzanych-zasobow-cyberataki/

Branecki K., *Analiza wektorów ataku i wycieków danych z Yahoo*, Sekurak, https://sekurak.pl/analiza-wyciekow-z-yahoo/

Branecki K., *Wyciek danych z Equifax – analiza anatomii ataku*, Sekurak, https://sekurak.pl/wyciek-danych-z-equifax-analiza/

Chrobot M., *Yahoo ukarane przez SEC za zatajenie ataku hakerskiego*, Komputer Świat, https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/yahoo-ukarane-przez-sec-za-zatajenie-ataku-hakerskiego/

Co to jest cyberatak?, Microsoft Security, https://www.microsoft.com/pl-pl/security/business/security-101/what-is-a-cyberattack

Cyberprzestępczość 2025: Jakie branże są najbardziej narażone na ataki hakerskie?, Bitdefender, https://bitdefender.pl/cyberprzestepczosc-2025-jakie-branze-sa-najbardziej-narazone-na-ataki-hakerskie/

Globalny koszt cyberataków w 2026 r., Blog ExpressVPN, https://www.expressvpn.com/pl/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/

Kaczmarek A., *Kary i ugody po wycieku w Equifax: finansowe skutki braku aktualizacji*, CyberDefence24, https://cyberdefence24.pl/polityka-i-prawo/kary-i-ugody-po-wycieku-w-equifax

Konieczny P., *Wszystkie 3 miliardy kont Yahoo zostało zhakowanych*, Niebezpiecznik, https://niebezpiecznik.pl/post/wszystkie-3-miliardy-kont-yahoo-zostalo-zhakowanych/

Kurek K., *Atak na SolarWinds. Jak doszło do największego włamania w historii?*, CyberDefence24, https://cyberdefence24.pl/cyberbezpieczenstwo/atak-na-solarwinds-jak-doszlo-do-najwiekszego-wlamania-w-historii

Maciejewski A., *Sunburst i konsekwencje ataku na łańcuch dostaw*, ITwiz, https://itwiz.pl/sunburst-i-konsekwencje-ataku-na-lancuch-dostaw/

Maciejewski A., *Wpływ naruszeń bezpieczeństwa na wycenę i przejęcie Yahoo przez Verizon*, ITwiz, https://itwiz.pl/wplyw-naruszen-bezpieczenstwa-na-wycene-i-przejecie-yahoo

Nachreiner C., *How a secure MFA would have avoided the Colonial cyberattack*, WatchGuard, https://www.watchguard.com/fr/wgrd-news/blog/how-secure-mfa-would-have-avoided-colonial-cyberattack

Piotrowski P., *Bezpieczeństwo łańcucha dostaw IT po incydencie SolarWinds*, Securitum, https://securitum.pl/bezpieczenstwo-lancucha-dostaw-it-po-incydencie-solarwinds

Piotrowski P., *Obrona w głąb jako fundament bezpieczeństwa IT*, Securitum, https://securitum.pl/obrona-w-glab-jako-fundament-bezpieczenstwa/

Profil cyberprzestępcy i metodyka ataków, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/cyberbezpieczenstwo

Redakcja CyberDefence24, *Prezes Colonial Pipeline potwierdza: zapłaciliśmy okup hakerom*, CyberDefence24, https://cyberdefence24.pl/biznes-i-finanse/prezes-colonial-pipeline-potwierdza-zaplacilismy-okup-hakerom

Redakcja Niebezpiecznik, *Ogromny wyciek z Equifax. 143 miliony Amerykanów straciło dane*, Niebezpiecznik.pl, https://niebezpiecznik.pl/post/ogromny-wyciek-z-equifax/

Redakcja PAP, *USA. Atak hakerski na sieć rurociągów Colonial Pipeline*, TVN24, https://tvn24.pl/swiat/usa-atak-hakerski-na-siec-rurociagow-colonial-pipeline-5090075

Redakcja Zaufana Trzecia Strona, *Jak doszło do włamania do Yahoo i kradzieży danych pół miliarda kont*, Zaufana Trzecia Strona, https://zaufanatrzeciastrona.pl/post/jak-doszlo-do-wlamania-do-yahoo-i-kradziezy-danych-pol-miliarda-kont/

Skomra W., Wojtasik K., *Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK*, E-journals Terroryzm, https://ejournals.eu/czasopismo/terroryzm/artykul/infrastruktura-krytyczna-jako-cel-dzialan-hybrydowych-studia-przypadkow-atakow-na-obiekty-i-systemy-ik

Smerdel P., *Informacje pozwalające na zrozumienie zagrożeń występujących w cyber-przestrzeni*, BIP Starostwo Powiatowe w Kwidzynie, https://bip.powiatkwidzynski.pl/artykul/informacje-pozwalajace-na-zrozumienie-zagrozen-wystepujacych-w-cyberprzestrzeni-oraz-porady-ja

Statystyki cyberbezpieczeństwa – najnowsze dane o cyberatakach 2025, Exorigo-Upos, https://www.exorigo-upos.pl/blog/statystyki-cyberbezpieczenstwa-dane-z-2025-roku/

Urbanek W., *Colonial Pipeline: niepożądana sława*, CRN Polska, https://crn.pl/artykuly/colonial-pipeline-niepozadana-slawa/

Inne

Computer Security Incident Handling Guide, National Institute of Standards and Technology (NIST), Washington 2012.

Krajobraz zagrożeń w cyberprzestrzeni. Raport roczny ENISA, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, 2024.

Report to Congressional Requesters. Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach, U.S. Government Accountability Office (GAO), Washington 2018.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP, Ministerstwo Cyfryzacji, Warszawa 2024.

Raport roczny z działalności CERT Polska w 2025 roku, NASK, Warszawa 2026.

Łukasz Karol BEŁCZOWSKI[1]

CYBERATAKI I ICH WPŁYW NA ESKALACJĘ KONFLIKTÓW MIĘDZYNARODOWYCH

Celem opracowania jest analiza operacyjnego i politycznego wymiaru cyberataków, z ograniczeniem szczegółowej warstwy technicznej. Szczególną uwagę poświęcono aspektom ideologicznym, które istotnie wpływają na działania podmiotów międzynarodowych we współczesnym środowisku bezpieczeństwa. Zjawiska te prowadzą do zwiększenia niepewności w zakresie identyfikacji sprawcy, co wpływa na sposób reakcji państw oraz zwiększa ryzyko eskalacji konfliktów. Uzyskane wyniki potwierdzają hipotezę, że cyberataki stanowią istotny komponent współczesnych konfliktów hybrydowych. W badaniu zastosowano metodę analizy studium przypadku, obejmującej wybrane incydenty cybernetyczne, w tym atak na Estonię w 2007 roku oraz incydent Sony Pictures z 2014 roku.

Słowa kluczowe: cyberwojna, cyberatak, bezpieczeństwo międzynarodowe, operacje w cyberprzestrzeni, konflikty międzynarodowe.

Wprowadzenie

Współczesne konflikty międzynarodowe w coraz większym stopniu uwzględniają znaczenie technologii telekomunikacyjnej, w tym mediów społecznościowych. Doktryna wojny hybrydowej definiowana jest jako zbiór działań łączących metody militarne oraz niemilitarne. Sama doktryna uwzględnia działania informacyjne, psychologiczne, ekonomiczne, społeczne, cybernetyczne a jej realizacja odbywa się przed etapem wypowiedzenia wojny[2]. Przykładem takich działań jest Federacja Rosyjska, która stosowała metody charakterystyczne dla wojny hybrydowej podczas inwazji na Ukrainę w 2014 roku[3].

Technologie cyfrowe pierwotnie nie posiadały wystarczającego bezpieczeństwa, co zostało wykorzystane przez podmioty, w tym państwa[4]. Pomimo istnienia mechanizmów bezpieczeństwa, takich jak szyfrowanie i audyty bezpieczeństwa, ich zakres implementacji jest zróżnicowany. Koszty i złożoność we wdrażaniu

---

[1] Łukasz Karol Bełczowski, student Politechniki Rzeszowskiej im. Ignacego Łukasiewicza, Koło Naukowe Polityki Bezpieczeństwa Państwa.

[2] E. Jakubiak, *Wojna hybrydowa jako nowy rodzaj konfliktu zbrojnego we współczesnym świecie*, „Zeszyt WAT" 2022, nr 24, s. 74-78.

[3] O. Polegkyi, *Rosyjska dezinformacja i propaganda przed i po inwazji na Ukrainę*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 2023, 21, z. 1. s. 92; E. Jakubiak, *Wojna hybrydowa…,* dz. cyt., s. 78-79.

[4] D.E. Sanger, *Cyberbroń – broń doskonała. Wojny, akty terroryzmu i zarządzanie strachem w epoce komputerów,* Helion S.A., Gliwice 2021, s. 9-23.

oraz trudność obsługi prowadzą do istotnych trudności, co skutkuje ograniczoną skutecznością ochrony.

Pomimo rosnącego znaczenia problematyki cyberataków w kontekście bezpieczeństwa międzynarodowego, zagadnienie to pozostaje fragmentarycznie opracowane[5]. Problem badawczy stanowi określenie charakteru i zakresu cyberataków oraz ich znaczenia dla funkcjonowania systemów bezpieczeństwa międzynarodowego.

W związku z tym sformułowano następujące pytania badawcze:

1. Jakie czynniki techniczno-polityczne ograniczają skuteczność oddziaływania cyberataków?
2. Jakie są różnice między uwarunkowaniami technicznymi a politycznymi?
3. W jaki sposób ograniczenia uwarunkowań wpływają na reakcję państw w środowisku międzynarodowym?

W prawie Unii Europejskiej brak jest legalnej definicji cyberprzestrzeni[6], jednak pojęcie to występuje niejawnie w regulacjach dotyczących bezpieczeństwa sieci i informacji, w szczególności w dyrektywie NIS2[7], gdzie akcentuje się ochronę infrastruktury cyfrowej jako elementu bezpieczeństwa państwa. W prawie polskim termin ten pojawia się m.in. w dokumentach strategicznych takich jak: „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej", w której cyberprzestrzeń ujmowana jest jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne oraz ich użytkowników.

W dokumentach poprzedniej strategii rządu Wielkiej Brytanii cyberprzestrzeń ujmowana była jako globalna przestrzeń systemów technologii informacyjnej powiązanych poprzez infrastrukturę sieciową, przy czym jej fundament stanowi Internet jako podstawowa platforma komunikacyjna[8]. Obecnie pojęcie to ujmowane jest w sposób bardziej funkcjonalny, jako środowisko obejmujące systemy teleinformatyczne, dane oraz usługi cyfrowe, których ochrona stanowi kluczowy element bezpieczeństwa narodowego i gospodarczego państwa. W dokumentach strategicznych podkreśla się przede wszystkim znaczenie odporności infrastruktury cyfrowej oraz zapewnienia ciągłości działania kluczowych usług, a nie samą definicję cyberprzestrzeni jako odrębnej kategorii pojęciowej[9].

Analiza powyższych ujęć wskazuje, że definicja amerykańska oraz brytyjska koncentrują się przede wszystkim na technologicznym i infrastrukturalnym wymiarze cyberprzestrzeni, podczas gdy podejście obecne w dokumentach europejskich – mimo braku definicji legalnej – rozszerza jej zakres o aspekty funkcjonalne i bezpieczeństwa systemowego.

---

[5] T. Rid, *Cyber War Will Not Take Place*, King's College London, UK 05 Oct 2011, s. 10-16.

[6] National Security Agency, https://www.nsa.gov/Press-Room/Speeches-Testimony/Article-View/Article/1624219/statement-for-the-record-by-lieutenant-general-keith-alexander-commander-joint (dostęp: 25.03.2026 r.).

[7] Dyrektywa NIS2 (UE) 2022/2555 (Dz.U. UE. L. 2022.333.80).

[8] UK Cyber Security Strategy, London 2011.

[9] Government Cyber Security Strategy 2022–2030, 25 January 2022.

Wojna hybrydowa – według Franka Hoffmana – oznacza „jednoczesne użycie wielu różnych typów działań zbrojnych przez elastycznych i wyrafinowanych przeciwników, którzy rozumieją, że skuteczny konflikt wymaga zastosowania różnych form walki dostosowanych do celów”[10]. W ujęciu tym kluczowe jest integrowanie metod konwencjonalnych (siły zbrojne) oraz niekonwencjonalnych (nieregularne formacje zbrojne, działania informacyjne, cyberoperacje) w ramach jednego konfliktu.

W podejściu instytucjonalnym NATO wskazuje, że zagrożenia hybrydowe obejmują skoordynowane wykorzystanie środków militarnych i niemilitarnych, zarówno jawnych, jak i ukrytych, w tym operacji dezinformacyjnych, cyberataków, nacisków ekonomicznych oraz działań paramilitarnych[11].

W literaturze występują jednak odmienne interpretacje tego pojęcia. Mark Galeotti podkreśla, że istotą działań hybrydowych jest przede wszystkim oddziaływanie informacyjne i manipulacja percepcją społeczną, a komponent militarny nie zawsze ma charakter dominujący[12]. Z kolei Lawrence Freedman wskazuje, że koncepcja wojny hybrydowej często pełni funkcję analityczną, służąc opisowi złożonych konfliktów współczesnych, lecz bywa krytykowana za nadmierną ogólność i brak precyzji definicyjnej[13].

Cyberwojna oznacza natomiast użycie operacji ofensywnych w ramach działań o charakterze polityczno-militarnym. Takie stanowisko reprezentuje Waldemar Krztoń[14]. Państwa lub zorganizowane grupy prowadzą koordynowane ataki cybernetyczne przeciwko przeciwnikowi, aby osiągnąć cele strategiczne (np. destabilizacja infrastruktury krytycznej, szpiegostwo technologiczne, czy propagandę w sieci). Działania te mogą nie być oficjalnie uznane za wojnę według tradycyjnej definicji, ale stanowią eskalację konfliktu w obszarze[15].

W literaturze przedmiotu brak jest jednak jednolitej definicji tego pojęcia[16]. Thomas Rid[17] wskazuje, iż wiele działań określanych mianem cyberwojny nie spełnia klasycznych kryteriów wojny, ponieważ nie prowadzi do bezpośredniej przemocy fizycznej, co podważa zasadność stosowania tego terminu. Odmiennie Lucas Kello[18] proponuje koncepcję „permanentnego konfliktu” (*unpeace*),

[10] G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, 2007, Potomac Institute for Policy Studies, Arlington, Virginia December 2007, s. 17.

[11] NATO, *Countering Hybrid Threats*, raporty i dokumenty strategiczne, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (dostęp: 22.04.2026 r.).

[12] M. Galeotti*, The Weaponisation of Everything: A Field Guide to the New Age of Global Conflict,* Yale University Press, 2023, s. 127-176.

[13] L. Freedman, *The Future of War: A History*, “PublicAffairs”, 10 października 2017 r., s. 32-44.

[14] W. Krztoń, *Wojna i konflikt zbrojny – przemiany,* „Obronność, Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej” 2013, nr 5, s. 143-154.

[15] M.B. Gazula, *Cyber Warfare Conflict Analysis and Case Studies*, Cambridge, maj 2017, https://web.mit.edu/smadnick/www/wp/2017-10.pdf, s. 13-17 (dostęp: 25.03.2026 r.).

[16] I. Oleksiewicz, M. Górka, *Bezpieczeństwo quasi militarne,* Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2022, s. 27.

[17] T. Rid, *Cyber War…,* dz. cyt., s. 10-16.

[18] L. Kello, *The Virtual Weapon and International Order*, Yale University Press 2017, s. 212-229.

sytuującego cyberoperacje pomiędzy stanem wojny a pokoju, jako nową kategorię relacji międzynarodowych.

W ujęciu instytucjonalnym NATO traktuje cyberprzestrzeń jako obszar operacyjny, w którym mogą być prowadzone działania o charakterze wojskowym, co implikuje możliwość uznania cyberataków za element konfliktu zbrojnego[19]. Ponadto cyberprzestrzeń ma stanowić kluczowe znaczenie do odstraszania i obrony przestrzeni kosmicznej oraz zapobiegania, wykrywania, przeciwdziałania i reagowania na szerokie spektrum zagrożeń. Cyberprzestrzeń to także przedmiot ciągłych sporów, w które ingerują aktorzy dążący do zniszczenia rządowej infrastruktury i przechwycenia intelektualnej własności oraz działań wojskowych[20]. Z kolei podejście prawne, rozwijane m.in. w ramach Tallinn Manual[21], wskazuje na trudności w kwalifikacji cyberataków jako użycia siły w rozumieniu prawa międzynarodowego, co wynika z problemów z atrybucją oraz oceną skutków takich działań.

Analiza powyższych ujęć wskazuje, że cyberkonflikt należy więc postrzegać jako zjawisko o charakterze hybrydowym, sytuujące się pomiędzy klasycznym konfliktem zbrojnym a działaniami poniżej progu wojny, co prowadzi do istotnych problemów definicyjnych i prawnych.

Analiza powyższych ujęć pozwala stwierdzić, że wojna hybrydowa stanowi model konfliktu wielowymiarowego, w którym dochodzi do integracji narzędzi militarnych, informacyjnych, ekonomicznych oraz cybernetycznych. Jej kluczową cechą jest rozmycie granic między wojną a pokojem oraz trudność w jednoznacznym przypisaniu odpowiedzialności, co generuje istotne wyzwania zarówno w wymiarze operacyjnym, jak i prawnym.

Przez pojęcie atrybucji cyberataków, zgodnie z ujęciem technicznym, należy rozumieć proces identyfikacji podmiotu odpowiedzialnego za dany incydent na podstawie analizy śladów cyfrowych oraz danych sieciowych[22]. Natomiast w ujęciu prawnym atrybucja oznacza przypisanie odpowiedzialności państwu lub innemu podmiotowi zgodnie z normami prawa międzynarodowego, co wymaga spełnienia określonych przesłanek, w szczególności wykazania kontroli nad sprawcą działania[23].

W literaturze podkreśla się, że atrybucja ma również wymiar polityczny. Joseph S. Nye Jr.[24] wskazuje, iż decyzja o przypisaniu odpowiedzialności za cyberatak często wykracza poza ustalenia techniczne i stanowi element strategii państwa. Atrybucja cyberataków obejmuje zatem wskazanie konkretnego sprawcy (np. państwa lub zorganizowanej grupy), jednak w praktyce jest to proces

[19] NATO, *Cyber defence,* https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence (dostęp: 22.04.2026 r.).

[20] Strategia NATO z 29 czerwca 2022 roku. https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept (dostęp: 22.04.2026 r.).

[21] M. Schmitt, *Tallinn Manual 2.0*, Cambridge University Press, 2017, s. 87.

[22] T. Rid, *Cyber War Will…,* dz. cyt., s. 8, 15, 16, 23.

[23] M. Schmitt, *Tallinn Manual 2.0…,* dz. cyt., s. 87.

[24] J.S. Nye Jr., *Deterrence and Dissuasion in Cyberspace*, "International Security" 2017, 41(3), s. 49-52.

wieloaspektowy – techniczny, prawny i polityczny – wymagający analizy dowodów oraz oceny ich wiarygodności. Jak wskazano w Tallinn Manual 2.0, przypisanie działania państwu wymaga m.in. ustalenia stopnia jego zaangażowania lub kontroli nad podmiotem dokonującym ataku[25]. Dokładna atrybucja cyberataków stanowi warunek konieczny podejmowania dalszych działań, w tym reakcji dyplomatycznych, sankcji lub środków odwetowych, jednak ze względu na złożoność środowiska cyberprzestrzeni często pozostaje obarczona znaczną niepewnością.

Studium przypadków operacji cybernetycznych

24 listopada 2014 roku systemy informatyczne Sony Pictures Entertainment padły ofiarą rozległego cyberataku, który w późniejszym okresie został przypisany przez FBI Korei Północnej[26]. Stało się to po opublikowaniu utworu filmowego „The Interview" („Wywiad ze słońcem narodu"), który był komedią satyryczną wyprodukowaną przez Amerykański koncern filmowy Sony Pictures Entertainment z udziałem scenarzystów Seth Rogen i Evan Goldberg246. Zapowiedź produkcji dzieła filmowego ogłoszono jeszcze w 2013 roku, a premierę zaplanowano na październik 2014 roku. Film przedstawiał historię dwóch dziennikarzy zwerbowanych przez Centralną Agencję Wywiadowczą (CIA), którzy zostają wysłani do Korei Północnej w celu przeprowadzenia zamachu na przywódcę państwa totalitarnego.

Pomimo rosnącego ryzyka eskalacji konfliktu międzynarodowego między Stanami Zjednoczonymi a Koreą Północną koncern filmowy Sony Pictures Entertainment nie podjął jakichkolwiek działań mających na celu wstrzymanie dystrybucji filmu utrzymując dotychczasowy plan premiery. Tego samego dnia pracownicy Sony Pictures Entertainment rozpoczęli dzień pracy w tygodniu poprzedzającym Święto Dziękczynienia w Stanach Zjednoczonych. Według relacji pracowników pojawiły się pierwsze nieprawidłowości w funkcjonowaniu systemów informatycznych, gdzie na monitorach wyświetlano obraz szkieletu z ostrym uzębieniem wraz z komunikatem skierowanym do pracowników[27]. Treść wiadomości miała charakter ultimatum i zawierała groźby ujawnienia poufnych danych przedsiębiorstwa filmowego poprzez udostępnienie ich w publicznym internecie. W komunikacie wskazano m.in.: „This is just the beginning" oraz „We've obtained all your internal data", co wskazuje na przestępczy charakter operacji hakerów. Za atakiem stała grupa "#GOP" (Guardians of Peace)[28].

---

[25] M. Schmitt, *Tallinn Manual 2.0…,* dz. cyt., s. 87.

[26] FBI National Press Office, *Update on Sony Investigation,* 19 grudnia 2014, https://www.fbi.gov/news/pressrel/press-eleases/update-on-sony-investigation (dostęp: 26.03.2026 r.).

[27] A. DeSimone, N. Horton, *Sony's Nightmare Before Christmas: The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace*. https://www.jhuapl.edu/sites/default/files/2022-12/SonyNightmareBeforeChristmas.pdf (dostęp: 19.04.2026 r.).

[28] Redaktor Niebezpiecznik.pl *Kto odpowiada za atak na SONY Pictures? Hipotezy mówią o Korei Północnej i Chinach, ale jest też wątek polski* https://niebezpiecznik.pl/post/kto-odpowiada-za-atak-na-sony-pictures-hipotezy-mowia-o-korei-polnocnej-i-chinach-ale-jest-tez-watek-polski/

Następnie, 27 listopada 2014 roku, pięć filmów Sony zostało upublicznionych bez jakiejkolwiek zgody firmy. Szacuje się, że utwory filmowe zostały pobrane na nielegalnych hostowanych serwisach internetowych. Wyciekły tytuły takie jak: "Brad Pitt's Fury", "Annie", "Mr. Turner", "Still Alice" oraz "To Write Love On Her Arms"[29].

W kolejnych dniach podjęto liczne działania mające na celu ograniczenie skutków incydentu. Zaangażowano prywatne firmy z sektora cyberbezpieczeństwa, m.in: Mandiant oraz Trend Micro. Analiza firm bezpieczeństwa cyfrowego wykazała, iż atak hakerski na Sony Pictures ma prawie identyczny charakter do wcześniejszych ataków pokroju "DarkSeoul", wraz z "Shamoon", które miały miejsce na terenie Korei Południowej. Na tej podstawie wysunięto hipotezę, że za atakiem stoi Korea Północna[30].

16 grudnia 2014 roku grupa „Guardians of Peace" skierowała liczne komunikaty do kin planujących wyświetlanie filmu „The Interview", w których zażądała niezwłocznego wycofania produkcji z dystrybucji. W komunikatach tych zawarto dodatkowo groźby, odwołujące się do ataków z 11 września 2001 roku (atak na World Trade Center), sugerując skrajne konsekwencje w przypadku niewycofania filmu. Rząd Stanów Zjednoczonych ze względu na groźby terroryzmu podejmuje szereg działań w tym zaangażowanie Federalnych, jak i Agencji Bezpieczeństwa Narodowego.

Ekspertyza FBI[31] wykazała, iż atakujący mieli dostęp do zasobów cyfrowych przed 24 listopada 2014 roku. Za najbardziej prawdopodobny scenariusz uznaje się atak phishingowy na jednego z nieuważnych pracowników Sony. Następnie atakujący analizowali możliwe scenariusze, szukali podatnych punktów oraz

(dostęp: 22.04.2026 r.); Federal Bureau of Investigation, *Update on Sony Investigation,* https://www.fbi.gov/news/press-releases/update-on-sony-investigation (dostęp: 19.04.2026 r.); Committee on Oversight and Government Reform, U.S. House of Representatives, *Letter to Michael Lynton regarding Sony Pictures Entertainment cyber attack*, December 23, 2014.

[29] D. Robb, *Sony Hack: A Timeline,* https://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ (dostęp: 18.03.2026 r.).
CNBC, Sony's new movies leak online following hack attack, https://www.cnbc.com/2014/11/30/sonys-new-movies-leak-online-following-hack-attack.html (dostep: 20.04.2026 r.).

[30] Cyberatak na Sony Pictures Entertainment wykazywał istotne podobieństwa do wcześniejszych operacji przypisywanych Korei Północnej, w szczególności do ataków „DarkSeoul" (2013) oraz „Shamoon". Podobieństwa te dotyczyły przede wszystkim zastosowania złośliwego oprogramowania typu „wiper", którego celem było trwałe usunięcie danych z systemów ofiary oraz uniemożliwienie ich dalszego funkcjonowania – Novetta, *Operation Blockbuster Report*, 2016 (dostęp: 20.04.2026 r.); *Analysis of wiper malware…* (SC Magazine), 2014, https://www.scworld.com/news/analysis-of-wiper-malware-implicated-in-sony-breach-exposes-shamoon-style-attacks?utm_source (dostęp: 20.04.2026 r.).
Redaktor Niebezpiecznik.pl *Kto odpowiada za atak na SONY Pictures? Hipotezy mówią o Korei Północnej i Chinach, ale jest też wątek polski…* https://niebezpiecznik.pl/post/kto-odpowiada-za-atak-na-sony-pictures-hipotezy-mowia-o-korei-polnocnej-i-chinach-ale-jest-tez-watek-polski/ (dostęp: 22.04.2026 r.).

[31] FBI National Press Office, *Update on Sony Investigation,* 19 grudnia 2014, https://www.fbi.gov/news/pressrel/press-eleases/update-on-sony-investigation (dostęp: 26.03.2026 r.).

zwiększali swój obszar działań, poprzez skanowanie sieci. Jak ustalili biegli, kradzież danych nie była jednym z celów atakujących. Głównym celem było zastraszenie Sony oraz uszkodzenie infrastruktury. Ekspertyza wykazała usunięcie partycji EFI z wielu komputerów, natomiast część danych została zmieniona w sposób nieodwracalny, uniemożliwiając poprawny odczyt. Złośliwe oprogramowanie wykorzystane w ataku miało charakter tzw. wipera, którego celem było trwałe usunięcie danych oraz zakłócenie funkcjonowania systemów informatycznych przedsiębiorstwa. Tego typu narzędzia są charakterystyczne dla operacji o wysokim poziomie destrukcyjności.

Cyberatak na Sony Pictures Entertainment z 2014 roku pozostaje kwestią sporną w kontekście przypisania odpowiedzialności. Federalne Biuro Śledcze (FBI), a następnie również Agencja Bezpieczeństwa Narodowego (NSA), wskazywały na zaangażowanie Korei Północnej w przeprowadzenie operacji.

Jednocześnie część analityków sektora cyberbezpieczeństwa podkreślała brak jednoznacznych dowodów technicznych potwierdzających tę hipotezę. Wskazywano również na możliwość manipulacji artefaktami cyfrowymi oraz ruchem sieciowym, co może utrudniać wiarygodną identyfikację sprawcy.

Eksperci tacy jak Bruce Schneier[32] zwracali uwagę, że choć kontekst polityczny może sugerować zaangażowanie Korei Północnej, dostępne dane techniczne nie pozwalają na jednoznaczne przypisanie odpowiedzialności konkretnemu państwu.

Cyberatak na Estonię w 2007 roku związany z pomnikiem „Brązowego Żołnierza"

Wiosną 2007 roku Estonia była jednym z najbardziej zinformatyzowanych społeczeństw w Europie – blisko 99% operacji bankowych odbywało się elektronicznie, funkcjonowało kilkaset e-usług publicznych, włącznie z internetowymi wyborami parlamentarnymi[33]. W tym czasie zaogniał się spór polityczny z Moskwą: w maju 2007 roku[34] rząd estoński zdecydował się przenieść z centrum Tallinna pomnik „Brązowego Żołnierza" – sowieckiego żołnierza z II wojny światowej – na cmentarz wojskowy. Dla estońskich Rosjan monument był symbolem „wyzwoliciela", dla wielu estońskich patriotów – „ciemiężyciela" – i stał się źródłem kilkunastu lat napięć wewnętrznych. Ogłoszenie planów przeniesienia pomnika doprowadziło do ulicznych protestów i ostrej retoryki władz rosyjskich

[32] B. Schneier, *Did North Korea Really Attack Sony?: It's Too Early to Take the U.S. Government at Its Word,* Atlantic, 22 grudnia 2014, http://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/ (dostęp: 26.03.2026 r.).

[33] H. Laasme, *Estonia: Cyber Window into the Future of NATO*, s. 59, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_58-63_Laasme.pdf?ver=Gmp2P_MaR_5WUw4ETKCnXA%3D%3D (dostęp: 25.03.2026 r.).

[34] T. Bielecki, *Nocna bitwa o historię.* gazeta.pl, 2007-04-28. https://web.archive.org/web/20070502061651/http://serwisy.gazeta.pl/swiat/1,34205,4097029.html (dostęp: 26.03.2026 r.).

(apel o bojkot estońskich towarów). To wydarzenie wytworzyło szeroki kontekst polityczno-geostrategiczny, w którym następnie wybuchły cyberataki – o szerokich cechach operacji informacyjnej ukierunkowanej na Estonię[35].

Ataki trwały 22 dni (od 27 kwietnia do 19 maja 2007 roku), a ich przebieg można podzielić na kilka faz:

- 27 kwietnia 2007 roku – rozpoczęła się pierwsza fala nieskoordynowanych ataków DDoS na wysoko postawione strony rządowe: witryny prezydenta, parlamentu, ministerstw, służb policyjnych, partii politycznych i głównych mediów,
- 4 maja 2007 roku – ruszyła druga, bardziej zaawansowana fala ataków. Oprócz wcześniejszych celów w ataku ucierpiały także duże banki komercyjne (m.in. Hansabank i SEB) oraz zaatakowano kluczowe usługi elektroniczne państwa,
- 9 maja 2007 roku – ataki osiągnęły apogeum. Data ta odpowiada obchodom Dnia Zwycięstwa w Rosji, co może wskazywać na symboliczny wymiar operacji,
- 19 maja 2007 roku – nastąpiło nagłe zakończenie operacji[36].

Technicznie, ataki polegały głównie na potężnych kampaniach DDoS – zalewaniu ofiar zapytaniami sieciowymi z sieci botnetów. Używano setek tysięcy, a według raportów nawet około miliona zainfekowanych komputerów na całym świecie (znaczna część „zombi" pochodziła ze Stanów Zjednoczonych). Atakom towarzyszyły także mniejsze operacje (np. masowe spamowanie), jednak największe zakłócenia dotyczyły zablokowania dostępu do portali rządowych, banków i mediów. Służby estońskie radziły sobie m.in. przez tymczasowe ograniczanie ruchu międzynarodowego (białe listy adresów) oraz współpracę CERT-EE z innymi zespołami reagowania na incydenty w Europie[37].

Dotychczas nie ustalono jednoznacznie, kto stał za atakami. Analiza ruchu wskazała na wyraźne elementy „rosyjskie": pakiety zawierały politycznie nacechowane frazy w języku rosyjskim (np. obraźliwe wyzwiska pod adresem ówczesnego premiera Andersa Ansipa), a instrukcje przeprowadzania ataków rozpowszechniane były na rosyjskojęzycznych forach internetowych. Mimo to żadna z grup hakerskich nie przyznała się oficjalnie do operacji. W styczniu 2008 roku estońskie sądy ukarały jedynie pojedynczego hakera – 20-letniego studenta Dmitrija Galuškevitša – który z Estonii zorganizował atak DDoS na stronę jednej z partii politycznych[38].

---

[35] R. Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,* https://www.researchgate.net/publication/279712069_Analysis_of_the_2007_cyber_attacks_against_estonia_from_the_information_warfare_perspective (dostęp: 25.03.2026 r.).

[36] Nato Strategic Communications of Center, *2007 cyberattacks on Estonia*, s. 59-61, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf (dostęp: 25.03.2026 r.).

[37] Nato Strategic Communications of Center, *2007 cyberattacks on Estonia,* s. 62.

[38] R. Ottis, *Analysis of the 2007…,* dz. cyt.

Wspólne śledztwo estońsko-rosyjskie zakończyło się fiaskiem: Rosja nie odpowiedziała na wniosek o pomoc prawną, mimo obowiązujących umów dwustronnych. Rząd Federacji Rosyjskiej zaprzeczał jakimkolwiek powiązaniom z atakiem. Brak bezpośrednich dowodów zmusił do opisania zdarzenia głównie w kategoriach „operacji informacyjnej" bądź „wojny hybrydowej" o proweniencji niepublicznej. W efekcie atrybucja pozostała niejasna – Estonii nie udało się ustalić, czy za atakiem stało rosyjskie państwo (w tajny sposób) czy jedynie niezależni prorosyjscy aktywiści.

W krótkim okresie ataki spowodowały poważne zakłócenia usług online i gospodarcze koszty – szacuje się straty w efektach produktywności i kosztach naprawy infrastruktury na setki milionów euro. Mimo dużej skali incydentu, estoński rząd i społeczeństwo zachowały względny spokój: szybka reakcja CERT, wsparcie międzynarodowe (większość państw NATO i UE pomogła przywracać usługi) oraz popularyzacja wówczas popularnego Skype'a umożliwiły skuteczne ograniczenie skutków incydentu.

Znacznie istotniejsze były jednak skutki długoterminowe. Atak na Estonię został odebrany jako „pierwszy udokumentowany w historii przypadek wojny informacyjnej na poziomie państwowym". NATO uznało incydent za sygnał ostrzegawczy i wyznaczające kierunek dla nowej polityki cyberbezpieczeństwa. Już w maju 2008 estoński rząd przyjął pierwszą[39] – czyniąc z obrony przed cyberatakami priorytet (sięgano nawet po cytat z incydentu). Również w tym okresie utworzono w Tallinnie NATO-wskie Centrum Doskonałości Obrony Cybernetycznej (CCDCOE). Atak przyczynił się do wzrostu świadomości wśród państw NATO/UE o zagrożeniach cyfrowych.

Podsumowanie

Współczesne konflikty międzynarodowe coraz częściej rozgrywają się w tzw. przestrzeni hybrydowej, gdzie cyberataki stają się pełnoprawnym narzędziem realizacji celów strategicznych państw. NATO zwraca uwagę, że zagrożenia hybrydowe łączą środki militarne i niemilitarne – w tym dezinformację oraz ataki cybernetyczne – które zamazują granicę między wojną a pokojem[40]. Dzięki temu państwa mogą wywierać presję polityczną i gospodarczą bez formalnego wypowiedzenia wojny. Przykładowo raport CyberPeace Institute pokazuje, że podczas inwazji na Ukrainę cyberoperacje były zsynchronizowane z działaniami militarnymi – cyberataki traktowano jak „pierwsze strzały", pełniące rolę mnożnika siły ofensywy[41].

---

[39] Pełna nazwa: Ministry of Defence of Estonia, *Cyber Security Strategy of Estonia 2008–2013*, Tallinn: Ministry of Defence, 2008.

[40] NATO, *Countering hybrid threats*, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (dostep: 26.03.2026 r.).

[41] M. Nedelcho, *Cyber Dimensions of a Hybrid Warfare*, 8 kwietnia 2025 roku, https://cyberpeaceinstitute.org/news/cyber-dimensions-of-a-hybrid-warfare (dostęp: 26.03.2026 r.).

Nie bez znaczenia pozostaje problem atrybucji cyberataków, który istotnie wpływa na ich znaczenie strategiczne. Trudno jednoznacznie ustalić sprawcę ataku, co sprawia, że agresorzy często pozostają bezkarni – klasyczne instrumenty prawa międzynarodowego czy sankcje nie zawsze mogą zostać zastosowane. W praktyce skutkuje to impasem: państwo-ofiara nie może łatwo udowodnić winy innego kraju, a co za tym idzie – uniknąć eskalacji. Przykładem jest estoński cyberatak z 2007 roku, który mimo znaczących szkód nie doprowadził do zastosowania artykułów 4 lub 5 Traktatu Północnoatlantyckiego[42]. Wówczas NATO nie zdecydowało, co podkreślono w analizach jako oznakę bezkarności autorów ataku[43]. Podobne trudności występują przy przypisywaniu autorstwa bardziej zaawansowanych cyberoperacji – dlatego niektóre ataki pozostają motywem do spekulacji, a ich analiza wymaga zaawansowanych środków śledczych i współpracy międzynarodowej.

Z perspektywy teoretycznej cyberataki redefiniują klasyczną dychotomię wojna–pokój, przesuwając konflikt na kontinuum działań wielowymiarowych. Współczesna rywalizacja obejmuje jednocześnie wiele wymiarów – od militarnego i cybernetycznego po informacyjny czy ekonomiczny – co sprawia, że działania agresywne trwają praktycznie bez przerwy, przechodząc płynnie od sabotażu do konwencjonalnych operacji. Jak zauważa Chris Demchak[44], „cyberowana" sfera konfliktu stała się permanentnym elementem globalnej walki o pozycję strategiczną, co prowadzi do sytuacji, w której wojna i pokój przenikają się nawzajem, tworząc ciągłe wyzwania dla bezpieczeństwa. W rezultacie tradycyjne modele bezpieczeństwa oparte na wyraźnym rozróżnieniu między stanem wojny i pokoju okazują się niewystarczające wobec natury współczesnych cyberzagrożeń.

Podsumowując, cyberataki są dziś integralnym elementem konfliktów międzynarodowych – ich zastosowanie w różnych wymiarach (technicznym, politycznym i informacyjnym) czyni z nich potężne narzędzie wpływu, którego rosnące znaczenie wymaga ciągłej adaptacji strategii obronnych i prawa międzynarodowego.

Bibliografia

Freedman L., *The Future of War: A History*, "PublicAffairs", 10 października 2017.

Galeotti M., *The Weaponisation of Everything: A Field Guide to the New Age of Global Conflict,* Yale University Press, 2023.

Hoffman G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, 2007, Potomac Institute for Policy Studies, Arlington, Virginia December 2007.

[42] Estonia: Cyber Window into the Future of NATO.

[43] Army University Press, *NATO's Cyber Era (1999–2024) Implications for Multidomain Operations*, https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/NATOs-Cyber-Era-UA (dostęp: 26.03.2026 r.).

[44] Ch. Demchak, *When Irregular Becomes Everywhere: The Cybered Fight in Unwanted Places*, https://mwi.westpoint.edu/when-irregular-becomes-everywhere-the-cybered-fight-in-unwanted-places/ (dostęp: 26.03.2026 r.).

Jakubiak E., *Wojna hybrydowa jako nowy rodzaj konfliktu zbrojnego we współczesnym świecie*, „Zeszyt WAT" 2022, nr 24.

Kello L., *The Virtual Weapon and International Order*, Yale University Press 2017.

Krztoń W., *Wojna i konflikt zbrojny – przemiany,* „Obronność, Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2013, nr 5.

Nye J.S. Jr., *Deterrence and Dissuasion in Cyberspace*, "International Security" 2017, 41(3).

Oleksiewicz I., Górka M., *Bezpieczeństwo quasi militarne,* Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2022.

Polegkyi O., *Rosyjska dezinformacja i propaganda przed i po inwazji na Ukrainę*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 2023, 21, z. 1.

Rid T., *Cyber War Will Not Take Place*, King's College London, UK 05 Oct 2011.

Sanger D.E., *Cyberbroń – broń doskonała. Wojny, akty terroryzmu i zarządzanie strachem w epoce komputerów,* Helion S.A., Gliwice 2021.

Schmitt M., *Tallinn Manual 2.0*, Cambridge University Press, 2017.

Prawodawstwo i dokumenty strategiczne

Cyber Security Strategy of Estonia 2008–2013, Ministry of Defence of Estonia, Tallinn 2008.

Dyrektywa NIS2 (UE) 2022/2555.

Government Cyber Security Strategy 2022–2030, London.

Strategia Cyberbezpieczeństwa RP 2019–2024.

Strategia NATO z 29 czerwca 2022 roku.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

UK Cyber Security Strategy, London 2011.

Government Cyber Security Strategy 2022–2030, 25 January 2022.

Netografia

Army University Press, *NATO's Cyber Era (1999–2024) Implications for Multidomain Operations*, https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/NATOs-Cyber-Era-UA

Bielecki T., *Nocna bitwa o historię.* gazeta.pl, https://web.archive.org/web/20070502061651/http://serwisy.gazeta.pl/swiat/1,34205,4097029.html

CNBC, *Sony's new movies leak online following hack attack*, https://www.cnbc.com/2014/11/30/sonys-new-movies-leak-online-following-hack-attack.html

Committee on Oversight and Government Reform, *Letter to Michael Lynton regarding Sony Pictures Entertainment cyber attack*, https://www.jhuapl.edu/sites/default/files/2022-12/SonyNightmareBeforeChristmas.pdf

Demchak Ch., *When Irregular Becomes Everywhere: The Cybered Fight in Unwanted Places*, https://mwi.westpoint.edu/when-irregular-becomes-everywhere-the-cybered-fight-in-unwanted-places/

DeSimone A., Horton N., *Sony's Nightmare Before Christmas: The 2014 North Korean Cyber Attack on Sony*, https://www.jhuapl.edu/sites/default/files/2022-12/SonyNightmare Before-Christmas.pdf

Federal Bureau of Investigation, *Update on Sony Investigation*, https://www.fbi.gov/news/press-releases/update-on-sony-investigation

Laasme H., *Estonia: Cyber Window into the Future of NATO*, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_58-63_Laasme.pdf

National Security Agency, *Statement for the Record by Lt. Gen. Keith Alexander*, dostęp online: https://www.nsa.gov/Press-Room/Speeches-Testimony/Article-View/Article/1624219/statement-for-the-record-by-lieutenant-general-keith-alexander-commander-joint

NATO, *Countering Hybrid Threats*, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

NATO, *Cyber Defence*, https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

Nato Strategic Communications Centre of Excellence, *2007 Cyberattacks on Estonia*, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

Nedelcho M., *Cyber Dimensions of a Hybrid Warfare*, https://cyberpeaceinstitute.org/news/cyber-dimensions-of-a-hybrid-warfare

Novetta, *Operation Blockbuster Report*, https://www.usna.edu/CyberCenter/_files/documents/Operation-Blockbuster-Report.pdf

Niebezpiecznik.pl *Kto odpowiada za atak na SONY Pictures? Hipotezy mówią o Korei Północnej i Chinach, ale jest też wątek polski…* https://niebezpiecznik.pl/post/kto-odpowiada-za-atak-na-sony-pictures-hipotezy-mowia-o-korei-polnocnej-i-chinach-ale-jest-tez-watek-polski/

Ottis R., *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Robb D., *Sony Hack: A Timeline*, https://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/

Schneier B., *Did North Korea Really Attack Sony?*, http://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/

SC Magazine, *Analysis of wiper malware implicated in Sony breach*, https://www.scworld.com/news/analysis-of-wiper-malware-implicated-in-sony-breach-exposes-shamoon-style-attacks

ZAKOŃCZENIE

Cechą wojny czy konfliktów zbrojnych jest asymetryczność. Co więcej, po rozpadzie zimnowojennego układu sił istotnym czynnikiem stają się aktorzy pozapaństwowi. Różne bowiem są ich cele, możliwości oraz implikacje. W kontekście „nowych wojen" cyberprzestrzeń przynosi wiele szans, co zagrożeń.

Źródeł wielu konfliktów należy szukać także w przeszłości kolonialnej, która pozostawiła po sobie liczne napięcia i nierozwiązane problemy. Często konflikty te mają również wymiar religijny, co dodatkowo wzmacnia ich intensywność i sprzyja pojawianiu się zjawisk takich jak terroryzm. Współczesne konflikty zbrojne ulegają coraz większej transformacji. Postęp technologiczny zredefiniował tradycyjne ujęcie konfliktu zbrojnego widzianego przez pryzmat Carl von Clausewitz, ponieważ bitwy nie są już definiowane wyłącznie przez działania militarne. Cyfryzacja wymusiła na nas stosowanie narzędzi cybernetycznych czy dronów, co spowodowało, że przemoc stała się bardziej dostępna. Cechą charakterystyczną tych konfliktów jest ich rozciągnięcie w czasie oraz zmienna intensywność. Mamy do czynienia z zupełnie nowymi wojnami – częściej są to konflikty trwające latami, które przechodzą różne fazy. W ich trakcie zmieniają się aktorzy, pojawiają się nowe grupy, a istniejące podlegają przemianom organizacyjnym, ideologicznym czy społecznym. Choć można uznać, że jeden konflikt składa się z wielu odrębnych epizodów, to jednak widoczna ciągłość i powiązania między nimi pozwalają traktować go jako całość. Wydaje się zatem, że przyszłe konflikty w cyberprzestrzeni będą więc charakteryzować się eskalacją asymetrycznych działań, w których przewaga nie będzie wynikać z liczebności, lecz z elastyczności, wiedzy specjalistycznej i możliwości wykorzystania zaawansowanych technologii.

Można wyróżnić pewien proces przechodzenia od konfliktów ukierunkowanych na przejęcie władzy lub kontroli nad terytorium, przez konflikty o charakterze kryminalnym, aż po stan przypominający chaos, w którym walczą ze sobą liczne, często zmieniające się podmioty.

Długotrwałość i niestabilność współczesnych konfliktów podważają tradycyjny podział na stan wojny i pokoju. W praktyce rzadko dochodzi do formalnego zakończenia konfliktu poprzez traktat pokojowy – częściej mamy do czynienia z zawieszeniem broni lub czasowym wyciszeniem walk, czego najlepszym przykładem jest trwająca wojna na Bliskim Wschodzie lub wojna ukraińsko-rosyjska. W związku z tym pojawia się koncepcja „nowych wojen", które można traktować jako odrębny stan pomiędzy wojną a pokojem, charakteryzujący się stałym napięciem i okresowymi wybuchami przemocy. Taka sytuacja rodzi poważne pytania o aktualność dotychczasowych pojęć, takich jak prawo wojenne czy suwerenność państwa. Trudno jednoznacznie określić, czym jest wojna, jeśli nie odpowiada ona

klasycznym definicjom, oraz jak rozumieć procesy przywracania pokoju. Dodatkowo rosnąca rola aktorów pozapaństwowych zmienia sposób funkcjonowania systemu międzynarodowego.

Izabela Oleksiewicz

Asymetryczność konfliktów w XXI wieku

Streszczenie

Współczesne spory międzynarodowe coraz częściej toczą się w tzw. przestrzeni hybrydowej, w której cyberataki stały się jednym z kluczowych narzędzi realizacji interesów strategicznych państw. Zagrożenia hybrydowe obejmują zarówno działania militarne, jak i niemilitarne, takie jak dezinformacja czy ataki w cyberprzestrzeni, przez co granica między stanem wojny a pokoju staje się coraz mniej wyraźna. Przyczyn wielu współczesnych konfliktów należy doszukiwać się także w wydarzeniach historycznych, które pozostawiły po sobie nierozwiązane problemy oraz napięcia. Obecnie, obok tradycyjnych konfliktów zbrojnych, istotną rolę odgrywają również konflikty społeczne, ekonomiczne, polityczne oraz cybernetyczne. Współczesne konflikty charakteryzują się również asymetrycznym charakterem. Po zakończeniu zimnej wojny coraz większe znaczenie zyskali także aktorzy pozapaństwowi, których cele, możliwości działania oraz skutki aktywności są bardzo zróżnicowane. Niniejsza publikacja stanowi próbę znalezienia odpowiedzi nie tylko na pytanie, czym jest konflikt i w jaki sposób ewoluuje, ale także jak istotną zmienną tych konfliktów jest asymetryczność.

The asymmetry of conflicts in the 21st century

Summary

Contemporary international disputes are increasingly taking place in what is known as the “hybrid domain”, where cyberattacks have become one of the key tools for advancing states' strategic interests. Hybrid threats encompass both military and non-military actions, such as disinformation or cyberattacks, making the line between war and peace increasingly blurred. The causes of many contemporary conflicts can also be traced back to historical events that left behind unresolved issues and tensions. Currently, alongside traditional armed conflicts, social, economic, political, and cyber conflicts also play a significant role. Contemporary conflicts are also characterized by their asymmetric nature. Following the end of the Cold War, non-state actors have also gained increasing significance, with their objectives, capabilities, and the effects of their activities varying widely. This publication attempts to answer not only the question of what conflict is and how it evolves, but also how asymmetry serves as a key variable in these conflicts.

DOCUMENT CREATED WITH

PDF COMBINER

PDF Combiner is a free application that you can use to combine multiple PDF documents into one.

Three simple steps are needed to merge several PDF documents. First, we must add files to the program. This can be done using the Add files button or by dragging files to the list via the Drag and Drop mechanism. Then you need to adjust the order of files if list order is not suitable. The last step is joining files. To do this, click button Combine PDFs.

Main features:

secure PDF merging - everything is done on your computer and documents are not sent anywhere

simplicity - you need to follow three steps to merge documents

possibility to rearrange document - change the order of merged documents and page selection

reliability - application is not modifying a content of merged documents.

Visit the homepage to download the application:

www.jankowskimichal.pl/pdf-combiner

To remove this page from your document, please donate a project.