„Polityka i Społeczeństwo" 1(21) / 2023
DOI: 10.15584/polispol.2023.1.20

ARTYKUŁY

Henryk Wyrębek*

ZAGROŻENIA HYBRYDOWE BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA

Streszczenie

Aneksja Krymu oraz początki rosyjskiej agresji w Donbasie zapoczątkowały szerokie wykorzystanie w dyskursie publicystycznym i rozważaniach naukowych pojęcia zagrożenia hybrydowe, które wiąże się z takimi zagrożeniami, jak rozpowszechnianie fałszywych informacji i manipulowanie nimi w sposób podważający zaufanie społeczeństwa do władzy oraz rozpowszechnianie informacji kompromitujących polityków. Podejmując próbę osłabienia umowy społecznej, która łączy państwo i jego wyborców, podmiot prowadzący działania hybrydowe próbuje podważyć zaufanie między instytucjami państwowymi a obywatelami. W rezultacie państwo traci swoją legitymizację – która jest w dużej mierze funkcją zaufania publicznego – a co za tym idzie, traci zdolność do działania, jak stwierdził Thomas Hobbes w 1651 roku w dziele *Lewiatan*. W konsekwencji grupa zagrożeń hybrydowych odnoszących się do działań informacyjnych niszczy zarówno fundamenty ideowe, jak i zdolność państwa do sprawnego funkcjonowania. W artykule podjęto próbę analizy i oceny istoty zagrożeń hybrydowych mających duży wpływ na obniżenie poziomu bezpieczeństwa informacyjnego państwa.

Słowa kluczowe: dezinformacja, przeciwdziałanie dezinformacji, *fake news*, *deepfake*, ataki hybrydowe, wojna hybrydowa

Wstęp

Postęp technologii informacyjnych, a wraz z nim zależność codziennego życia od Internetu prowadzi do powstania wielu nowych wyzwań i zagrożeń w cyberprzestrzeni[1]. Osiągnięcia technologiczne otworzyły nowe horyzonty i stworzyły różnorodne formy interakcji międzyludzkich, natomiast istotne zmiany społeczne wywierają wpływ na procesy

* Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, e-mail: henryk.wyrebek @uph.edu.pl, ORCID: 0000-0001-9801-6905.

[1] M. Górka, *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa* [w:] *Cyberbezpieczeństwo wyzwaniem XXI wieku*, red. T.R. Dębowski, Wrocław 2018, s. 31. Por. K. Michalski, M. Jurgilewicz, *Konflikty technologiczne. Nowa architektura zagrożeń w epoce wielkich wyzwań*, Warszawa 2022, s. 11 i n.

polityczne i sposób rządzenia społeczeństwem. Szybki rozwój technologiczny i ekonomiczny, zwiększający się zakres globalizacji, zanik tradycyjnych granic – to niektóre z wielu czynników powodujących wzrost zagrożeń bezpieczeństwa[2]. Wizja społeczeństwa informacyjnego jest zajmująca i wymaga fundamentalnych zmian w sposobach myślenia na temat jego funkcjonowania i rozwoju[3]. Tworzący się nowy paradygmat społeczeństwa informacyjnego skłania do poszukiwania i projektowania coraz doskonalszych rozwiązań informatycznych, które pozwolą kreować i doskonalić społeczeństwa[4]. Pojawiające się zagrożenia w cyberprzestrzeni ustanowiły, odmienne od obecnych, wymagania dotyczące bezpieczeństwa państwa. Cyberprzestrzeń stała się nowym środowiskiem bezpieczeństwa, co pociąga za sobą konieczność dokonania licznych zmian zarówno w pragmatyce, jak i w prawno-organizacyjnym wymiarze funkcjonowania systemów bezpieczeństwa. Rozwój nowoczesnych technologii wymusił znaczące przeobrażenia gospodarcze, społeczne, kulturowe i polityczne, wskazując na realne zmniejszenie znaczenia przypisywanego dobrom materialnym i kapitałom, przy jednoczesnym wzroście znaczenia niematerialnych czynników, tj. informacji i wiedzy[5]. W tym kontekście szczególnie istotne jest zrozumienie ważności bezpieczeństwa informacyjnego, które jest podstawą sprawnego funkcjonowania systemów państwa oraz wszystkich instytucji gospodarczych i pozagospodarczych[6]. Próby zinterpretowania pojęcia bezpieczeństwa informacyjnego są odzwierciedleniem wzrostu zainteresowania tą problematyką, wynikającego z narastających zagrożeń w przestrzeni informacyjnej państwa. Zagadnienia bezpieczeństwa informacyjnego państwa stają się ważnym obszarem badawczym współczesnych nauk o bezpieczeństwie.

---

[2] Z. Ciekanowski, J. Nowicka, H. Wyrębek, *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń,* Siedlce 2017, s. 104. Zob. A. Supel [i in.], *Edukacja i wychowanie na rzecz bezpieczeństwa i obronności – wybrane aspekty*, „Polityka i Społeczeństwo", 2022, nr 3, s. 180 i n.; M. Barć, *Planning and Organising Protection of Critical Infrastructure*, „Polityka i Społeczeństwo", 2022, nr 2, s. 5 i n.

[3] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* „Bezpieczeństwo Narodowe", 2012, nr 22, s. 138.

[4] H. Wyrębek, *Cyberprzestrzeń. Zagrożenia. Strategie bezpieczeństwa,* Siedlce 2021, s. 7.

[5] M. Golka, *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Warszawa 2008, s. 36.

[6] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, red. S. Sulowski, M. Brzeziński, Warszawa 2009. Por. m.in. M. Jurgilewicz, *Rola terenowych organów administracji publicznej w zapewnianiu bezpieczeństwa i porządku publicznego*, Warszawa 2023, s. 45 i n.; M.J. Bednarski, *Policja a środki masowego przekazu. Wybrane aspekty prawne*, Warszawa 2013, s. 35 i n.

Sytuacja problemowa, którą przedstawiono powyżej, określa problem badawczy sprowadzający się do odpowiedzi na pytanie: jakie zagrożenia hybrydowe bezpieczeństwa informacyjnego występują we współczesnym państwie i jakie działania zmierzające do ich minimalizacji podejmują organizacje międzynarodowe? Przyjmując powyższy problem naukowy do realizacji, nakreślony został cel niniejszych rozważań, który sprowadzał się do zidentyfikowania obszarów występowania zagrożeń hybrydowych, które wpływają na poziom bezpieczeństwa informacyjnego państwa. Wykonanie założonego celu badawczego było możliwe dzięki realizacji celów cząstkowych w obszarze teoriopoznawczym oraz badawczym. Celem teorio-poznawczym była analiza literatury przedmiotu i opracowań naukowych w zakresie występowania zagrożeń hybrydowych. Celem badawczym było zidentyfikowanie sposobów redukcji wpływu zagrożeń hybrydowych na bezpieczeństwo informacyjne państwa. Stąd też istotna w tym względzie była ocena inicjatyw NATO i Unii Europejskiej w tym zakresie. Bezpieczeństwo informacyjne zawsze jest obecne w polityce bezpieczeństwa i obronności państwa. Nie jest nową dziedziną bezpieczeństwa państwa, łączy procedury i narzędzia ochrony danych, informacji i systemów. Istotny jest również postęp naukowo-techniczny, który jest adaptowany na potrzeby ochrony informacji nie tylko z punktu widzenia jego użyteczności, ale także ze względu na przeciwdziałanie zagrożeniom[7].

Bezpieczeństwo informacyjne jest zbiorem działań, metod, procedur podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem[8]. Natomiast w projekcie doktryny bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej bezpieczeństwo informacyjne państwa postrzegane jest jako proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze[9].

S. Kowalkowski bezpieczeństwo informacyjne odnosi do wzrostu znaczenia informacji w zachowaniu stabilności współczesnych między-

[7] A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki Kolegium Analiz Ekonomicznych", 2013, nr 29, s. 452.

[8] P. Potejko, *Bezpieczeństwo informacyjne* [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Warszawa 2009, s. 194.

[9] *Projekt Doktryny bezpieczeństwa informacyjnego RP*, BBN 2015.

narodowych systemów ekonomicznych oraz zabezpieczeń przed atakami sieciowymi, a także skutkami ataków fizycznych[10].

Według E. Nowaka i M. Nowaka bezpieczeństwo informacyjne to stan warunków zewnętrznych i wewnętrznych umożliwiających państwu niezakłócony rozwój społeczeństwa informacyjnego, z następującymi warunkami zapewniającymi bezpieczeństwo informacyjne: niezagrożone strategiczne zasoby państwa; decyzje organów władzy podjęte na podstawie wiarygodnych, istotnych informacji; niezakłócony przepływ informacji pomiędzy organami państwa; niezakłócone funkcjonowanie sieci teleinformatycznych tworzących krytyczną infrastrukturę teleinformatyczną państwa; zagwarantowaną przez państwo ochronę informacji niejawnych i danych osobowych obywateli; zasadę, że prawo do prywatności obywateli jest nienaruszane przez instytucje publiczne, swobodny dostęp obywateli do informacji publicznej[11]. Bezpieczeństwo informacyjne jest jednym z najważniejszych przejawów bezpieczeństwa międzynarodowego i narodowego[12].

Dla zapewnienia wysokiego poziomu bezpieczeństwa informacyjnego i tym samym niezakłóconego funkcjonowania systemu informacyjnego państwa niezbędna jest identyfikacja, analiza i ocena jego zagrożeń. W literaturze przedmiotu można spotkać różne określenia dotyczące tego pojęcia. Współcześnie zagrożenia zmieniają swój charakter i związane z nim wyzwania dla bezpieczeństwa. Niektóre zagrożenia zanikają, jeszcze inne trwają nadal albo wyłaniają się ze zwiększoną siłą[13].

K. Liderman zagrożenia bezpieczeństwa informacyjnego odnosi do: sił natury (pożar, powódź, huragan, trzęsienie ziemi, epidemie); błędów ludzkich i ich działań wg błędnych lub niewłaściwych procedur; celowych, szkodliwych działań ludzi; awarii sprzętu komputerowego; awarii oprogramowania; awarii infrastruktury usługowej (zasilania, klimatyzacji, wody, ogrzewania)[14]. Natomiast P. Bączek zagrożenia bezpieczeństwa informacyjnego dzieli na: zagrożenia losowe – klęski żywiołowe, katastrofy, wypadki, które wpływają na stan bezpieczeństwa informacyj-

[10] *Niemilitarne zagrożenia bezpieczeństwa publicznego*, red. S. Kowalkowski, Warszawa 2011, s. 13.

[11] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 103.

[12] J. Nowicka, H. Elak, Z. Ciekanowski, *Bezpieczeństwo jako kategoria funkcjonowania państwa* [w:] *Współczesne zagrożenia bezpieczeństwa państwa*, red. Z. Ciekanowski, cz. II, Biała Podlaska 2021, s. 168.

[13] H. Wyrębek, *National security challenges and threats*, „Wiedza Obronna", 2022, nr 2, s. 117.

[14] K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017, s. 43.

nego organizacji (np. pożar budynku, w którym przechowywane są nośniki informacji); tradycyjne zagrożenia informacyjne – szpiegostwo, działalność dywersyjna lub sabotażowa, ofensywa dezinformacyjna prowadzona przez obce państwa lub osoby, podmioty, organizacje; zagrożenia technologiczne – zagrożenia związane z gromadzeniem, przetwarzaniem i przekazywaniem informacji w sieciach teleinformatycznych (do takich zagrożeń zaliczamy przestępstwa komputerowe, cyberterroryzm, walkę informacyjną); zagrożenia odnoszące się do praw obywatelskich osób lub grup społecznych, m.in. sprzedaży informacji, przekazywania informacji podmiotom nieuprawnionym, naruszania przez władze prywatności, bezprawnych ingerencji służb specjalnych, ograniczenia jawności życia publicznego[15].

Poważnym zagrożeniem dla bezpieczeństwa informacyjnego państwa są organizacje terrorystyczne, które oprócz tradycyjnych form wywierania przymusu coraz częściej prowadzą ataki technocyberterrorystyczne, a także operacje psychologiczne w środkach masowego przekazu, propagując fałszywe lub sprzeczne informacje, rozsiewając lęk, niepewność, wątpliwości, a w zglobalizowanym świecie cyfrowych technologii, w którym czynnik odległości traci znaczenie, obrazy prezentowane przez elektroniczne media często już teraz kreują specyficzne wrażenie więzi pomiędzy ofiarami ataków terrorystycznych a odbiorcami przekazywanych informacji[16]. Zagrożeniem dla bezpieczeństwa informacyjnego jest także aktywność grup, środowisk, firm, koncernów, które w swojej działalności świadomie manipulują przekazem informacji, maskując swoje prawdziwe cele, wykorzystując techniki manipulacji, perswazji, dezinformacji, propagandy[17]. Dużym wyzwaniem w obszarze zapewnienia wysokiego poziomu bezpieczeństwa informacyjnego państwa są zagrożenia hybrydowe.

Zagrożenia hybrydowe

Zagrożenia hybrydowe obejmują szeroki obszar działań destabilizujących bezpieczeństwo informacyjne państwa. Unia Europejska zagrożenia hybrydowe definiuje jako połączenie działań konwencjonalnych

[15] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 73.

[16] R. Borkowski, *Fabryki strachu – obraz terroryzmu jako kicz w medialnej popkulturze. Zagrożenia bezpieczeństwa międzynarodowego* [w:] *Analiza informacji. Teoria i praktyka*, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2012., s. 113.

[17] L. Więcaszek-Kuczyńska, *Zagrożenia bezpieczeństwa informacyjnego*, „Obronność. Zeszyty Naukowe", 2014, nr 2, s. 222.

i niekonwencjonalnych (militarnych i niemilitarnych), stosowanych w skoordynowany sposób przez aktorów państwowych i niepaństwowych, ukierunkowanych na osiągnięcie celów politycznych. UE podkreśla wielowymiarowość zagrożeń hybrydowych wykorzystujących środki przymusu i dywersyjne wymierzone w krytyczne słabe punkty. Zagrożenia hybrydowe rozciągają się od ataków cybernetycznych na krytyczne systemy informacyjne, przez zakłócanie usług krytycznych, do podważania zaufania społecznego do instytucji rządowych i pogłębiania podziałów społecznych[18].

Typowe zagrożenia hybrydowe można wyodrębnić w pięciu głównych grupach działań. Są to działania: regularne, nieregularne, informacyjne, ekonomiczne i polityczne.

W działaniach regularnych biorą udział siły zbrojne, prywatne firmy militarne oraz służby specjalne. Są to operacje specjalne, działania niekonwencjonalne, inwigilacja struktur i służb państwowych oraz zastraszanie przez demonstrację siły i zajmowanie terenu pod pretekstem przywracania pokoju. Działania nieregularne prowadzone są przez grupy niezadowolenia społecznego, mniejszości etniczne, grupy przestępcze, organizacje terrorystyczne. Jest to siłowe przejmowanie obiektów, tworzenie samozwańczych władz jako alternatywy dla tych funkcjonujących legalnie oraz akty nieposłuszeństwa obywatelskiego.

Grupa działań informacyjnych realizowana jest przez środki masowego przekazu, rozgłośnie radiowe należące do sił zbrojnych i służb specjalnych oraz cyberprzestępców i cyberterrorystów, z zagrożeniami takimi, jak: rozpowszechnianie *fake news*, fałszywych informacji, dezinformacji z manipulowaniem informacjami w sposób podważający zaufanie społeczeństwa do władzy, rozpowszechnianie informacji kompromitujących polityków, ataki cybernetyczne na serwery rządowe i samorządowe, cyberprzestępstwa. Szczególnym przykładem dezinformacyjnego manipulowania treścią jest coraz częściej pojawiające się w przestrzeni publicznej zjawisko zwane *deepfake* (z ang., w znaczeniu głęboki fałsz). Polega ono na łączeniu i nakładaniu nieruchomych lub ruchomych obrazów na obrazy źródłowe przy użyciu uczących się systemów komputerowych. Uzyskane w ten sposób łudząco realistyczne przekazy filmowe stwarzają możliwość głębokiej manipulacji na przykład poprzez zamianę twarzy prezentowanych postaci[19].

Działania ekonomiczne są realizowane przez polityków, urzędników i banki, głównie poprzez groźbę lub nagłe wstrzymanie dostaw surow-

[18] P. Szymański, *NATO i Unia Europejska wobec zagrożeń hybrydowych,* Ośrodek Studiów Wschodnich, https://www.osw.waw.pl, 24.04.2020 (20.02.2023).

[19] *Fake news – dezinformacja online*, Warszawa 2020, s. 9.

ców czy produktów. Działania polityczne przejawiają się w postaci finansowania grup niezadowolenia społecznego i mniejszości etnicznych, nadawania podwójnego obywatelstwa oraz wydawania paszportów agresora, korumpowania osób o wysokiej pozycji społecznej oraz podważania na arenie międzynarodowej legitymizacji sprawowania rządów przez władze. Realizowane są przez polityków, dyplomatów, urzędników, biznesmenów i służby specjalne.

W kolejnych latach należy spodziewać się dalszego wzrostu znaczenia zagrożeń hybrydowych dla bezpieczeństwa Polski i krajów NATO. Dezinformacja, cyberataki, działalność wywrotowa i konflikty o niskiej intensywności zostaną zaostrzone przez postępującą rewolucję technologiczną i globalną łączność[20]. Zagrożeniem dla bezpieczeństwa informacyjnego są w szerszej skali wojny hybrydowe.

Wojna hybrydowa

Twórcami koncepcji wojny hybrydowej są amerykańscy analitycy wojskowi. Miała być ona odpowiedzią na doświadczenia zdobyte przez armię Stanów Zjednoczonych w konfliktach w Afganistanie i Iraku oraz w tzw. wojnie z terroryzmem, a także próbą nowego podejścia teoretycznego, które będzie skuteczniej wyjaśniać otaczającą rzeczywistość. Wojna hybrydowa różni się od wojny klasycznej tym, że dla osiągnięcia przewagi nad przeciwnikiem jest wykorzystywana nie tylko siła militarna, ale także metody walki informacyjnej, propagandy i działań wywrotowych.

Ponadto podejmowane są próby destrukcyjnego wpływu na opinię publiczną, wspierania antysystemowych sił politycznych i radykalnych ruchów społecznych, ingerowania w systemy informatyczne organów władzy państwowej oraz firm prywatnych.

Terminem wojny hybrydowe w dyskursie naukowym już w latach 90. XX wieku posługiwał się Thomas R. Mockaitis[21].

Działania hybrydowe oraz wojnę hybrydową opisał w 2002 roku William Nemeth w pracy poświęconej analizie konfliktu rosyjsko-

[20] T. Kijewski, *Znaczenie zagrożeń hybrydowych dla bezpieczeństwa Polski i państw NATO*, The Warsaw Institute Review, https://warsawinstitute.org, 16.02.2023 (20.02.2023).

[21] A. Krzak, *Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego,* „Przegląd Bezpieczeństwa Wewnętrznego", 2018, nr 18, s. 17; T.R. Mockaitis, *British Counterinsurgency in the Post-imperial Era*, London 1995, s. 16–38.

czeczeńskiego[22]. Autor zamieścił w niej pojęcie hybrydowości nie tylko w stosunku do działań prowadzonych przez czeczeńskich bojowników, lecz także do sposobu funkcjonowania tamtejszego społeczeństwa. Jedną z cech społeczeństwa hybrydowego jest połączenie nowoczesnych teorii politycznych z tradycyjną organizacją społeczną i obyczajowością. Hybrydowy kształt danego społeczeństwa ma bezpośrednie przełożenie na sposób prowadzenia przez nie wojny[23].

Według F.G. Hoffmana konflikty hybrydowe mogą być prowadzone zarówno przez państwa, jak i podmioty pozapaństwowe[24]. Ponadto operacje hybrydowe mogą być realizowane przez pojedyncze oddziały lub ich większe zgrupowania. Ich działania są koordynowane w ramach jednego, głównego pola walki, po to, aby uzyskać efekt synergii. Zwycięstwo w wojnie hybrydowej ma być osiągnięte przede wszystkim przez połączenie wykorzystania nowoczesnych technologii wojskowych z taktyką działań partyzanckich. Hoffman zwraca również uwagę na znaczenie aktywności przestępczej, która ma zwiększać chaos i proces rozkładu atakowanego państwa.

Kierując się opracowaną definicją, Hoffman i jego współpracownicy przestudiowali historyczne konflikty zbrojne. Ostatecznie uwagę skupiono na II wojnie w Libanie w 2006 roku pomiędzy armią izraelską a Hezbollahem. Konflikt ten został uznany za najlepszy przykład wojny hybrydowej. Przesądziły o tym jego następujące cechy[25]:

- zdolność podmiotu pozapaństwowego do rzucenia wyzwania militarnego zachodniemu modelowi prowadzenia działań zbrojnych,
- sposób koordynowania operacji zdecentralizowanych komórek bojowych przez kierownictwo Hezbollahu,
- wysoki poziom przeszkolenia wojskowego oddziałów Hezbollahu,
- wykorzystanie przez oddziały Hezbollahu obszarów miejskich do unikania ich wykrycia oraz organizowania zasadzek,
- zdolność obsługi przez bojowników Hezbollahu nowoczesnego sprzętu wojskowego, w tym rakietowych pocisków przeciwokrętowych oraz przeciwpancernych,
- umiejętność wtapiania się żołnierzy Hezbollahu w ludność cywilną,

[22] Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia,* „Przegląd Bezpieczeństwa Wewnętrznego", 2016, nr 14, s. 40.

[23] W.J. Nemeth, *Future war and Chechnya: A case for hybrid warfare*, Monterey 2002, Calhoun: Naval Postgraduate School, http://calhoun.nps.edu, 1.06.2002 (5.02.2023).

[24] F.G. Hoffman, *Hybrid Warfare and Challenges*, „Joint Force Quarterly", 2009, nr 52, s. 34.

[25] Ł. Skoneczny, *op.cit.*, s. 43.

– prowadzenie przez Hezbollah działań informacyjno-wywiadowczych realizowanych na poziomie strategicznym oraz operacyjnym (np. wykorzystanie nowoczesnego sprzętu do podsłuchiwania rozmów izraelskich żołnierzy prowadzonych przez telefony komórkowe).

Istnieją dwie wyraźne cechy charakterystyczne wojny hybrydowej. Granica między wojną a pokojem zostaje zamazana. Oznacza to, że trudno jest zidentyfikować lub rozróżnić próg działań zbrojnych. Pojęcie wojny staje się nieuchwytne, ponieważ trudno je przełożyć na konkretne realia. Wojna hybrydowa poniżej progu działań zbrojnych lub bezpośredniej, jawnej agresji przynosi korzyści, gdyż jest łatwiejsza, tańsza i mniej ryzykowna niż operacje kinetyczne.

O wiele bardziej wykonalne jest szerzenie dezinformacji we współpracy z podmiotami niepaństwowymi niż wjechanie czołgami na terytorium innego kraju lub wprowadzenie myśliwców w jego przestrzeń powietrzną. Koszty i ryzyko są znacznie mniejsze, ale szkody są realne. Można prowadzić wojnę bez bezpośredniej walki lub fizycznej konfrontacji. Pozostaje to również w ścisłym związku z filozofią wojny.

Najwyższą sztuką wojenną jest pokonanie wroga bez walki, jak sugerował chiński starożytny strateg wojskowy Sun Tsu[26]. Drugą cechą charakterystyczną wojny hybrydowej jest niejednoznaczność i kwestia przypisania odpowiedzialności. Ataki hybrydowe charakteryzują się na ogół dużą niejasnością. Niejasność ta jest świadomie tworzona i pogłębiana przez podmioty podejmujące działania hybrydowe. Państwo, które jest celem ataku, albo nie jest w stanie wykryć ataku hybrydowego, albo nie jest w stanie przypisać go państwu, które być może przeprowadziło go lub sponsorowało. Pierwszym warunkiem skuteczności wojny hybrydowej, który musi zostać spełniony, jest kryzys w państwie będącym celem ataku. Wśród cech szczególnych oznak kryzysu można wskazać na[27]:

– złe funkcjonowanie administracji państwowej, wojska oraz służb bezpieczeństwa,
– istnienie silnych grup interesów, które realizują swoje partykularne cele, osłabiając tym samym politykę prowadzoną przez władze centralne i integralność całego państwa,
– duży poziom niezadowolenia z władz państwowych. U jego podstaw może leżeć konflikt na tle politycznym, etnicznym lub religijnym.

Kolejnym warunkiem koniecznym do skutecznego prowadzenia wojny hybrydowej jest istnienie na terenie państwa atakowanego mniejszości narodowych lub religijnych, które utożsamiają się z agresorem. Ważnym czynnikiem jest możliwość dotarcia z przekazem propagando-

[26] Sun Tzu, *Sztuka wojny*, Warszawa 2021, s. 24.
[27] Ł. Skoneczny, *op.cit*., s. 49.

wym do społeczeństwa państwa atakowanego. C. von Clausewitz twierdził, że „wojna jest tylko kontynuacją polityki innymi środkami". Choć może to być nadal prawdą, środki wojenne uległy znacznemu rozszerzeniu wraz z pojawieniem się współczesnych wojen hybrydowych. Oznacza to, że związek polityka – wojna stał się jeszcze bardziej złożony, ponieważ dynamika wojny podlega ciągłym zmianom. Wojna oznacza obecnie szereg możliwości. Czasami może ona pociągać za sobą operacje kinetyczne w połączeniu z wykorzystaniem podmiotów niepaństwowych. Może także obejmować ataki cybernetyczne wymierzone w infrastrukturę krytyczną oraz kampanie dezinformacyjne. Możliwości jest wiele, podobnie jak metod ich łączenia i zestawiania.

Wojna hybrydowa sprawia, że dynamika konfliktu staje się niejasna nie tylko dlatego, że oferuje szeroki i stale rosnący zestaw narzędzi do osłabiania przeciwnika, ale również dlatego, że pozwala na podważenie jego bezpieczeństwa militarnego na dwóch poziomach jednocześnie. Odnosi się to również do nadrzędnych celów wojny hybrydowej. Na poziomie potencjałów słabości atakowanego państwa w sferze politycznej, militarnej, gospodarczej, społecznej, informacyjnej i infrastrukturalnej są wykorzystywane tak, że prowadzi to do ich funkcjonalnego pogłębienia.

Drugi poziom, na którym podważane jest bezpieczeństwo państwa, ma charakter ideologiczny i odnosi się do legitymizacji państwa. Jak zauważa Norweska Agencja Współpracy na Rzecz Rozwoju, legitymizacja państwa dotyczy samej podstawy, na której państwo i społeczeństwo są wzajemnie powiązane i dzięki której władza państwowa jest prawomocna. Legitymizacja jest zatem nieodłączną podstawą władzy i praworządności państwa.

Działania hybrydowe są często ukierunkowane na słabe punkty atakowanego państwa lub międzypaństwowych wspólnot politycznych. Celem jest wykorzystanie tych słabości, pogłębiając je tak, aby stwarzać i zaostrzać polaryzację zarówno na poziomie krajowym, jak i międzynarodowym. Przekłada się to na niebezpieczną erozję podstawowych wartości współistnienia, harmonii i pluralizmu w społeczeństwach demokratycznych i pomiędzy nimi, a także zdolności przywódców politycznych do podejmowania decyzji. W ostatecznym rozrachunku zagrożenia hybrydowe znacznie obniżają poziom bezpieczeństwa informacyjnego państwa. Problematyka wojny hybrydowej jest przedmiotem szerokich badań. Mimo to pojęcie wojny hybrydowej nie zostało ostatecznie doprecyzowane na tyle, aby nie budziło kontrowersji wśród badaczy. Badaniami w tym zakresie zajmowali się m.in. William J. Nemeth, Frank Hoffmann, Nathan P. Freier[28].

[28] N.J. Newman, *Asymmetric Threats to British Military Intervention Operations*, London 2000; F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*,

Zwalczanie zagrożeń hybrydowych

Ważną rolę w zwalczaniu zagrożeń hybrydowych odgrywają państwa członkowskie NATO i UE. Rządy dysponują odpowiednimi zasobami w postaci wyspecjalizowanych struktur wywiadowczych, kontrwywiadowczych i rozpoznania wojskowego wspieranych przez instytucje odpowiedzialne za przestrzeganie porządku publicznego, narzędzi komunikacji z obywatelami czy zdolności do reagowania na incydenty w cyberprzestrzeni[29].

Od 2016 roku NATO i Unia Europejska identyfikują zwalczanie zagrożeń hybrydowych jako priorytet ich współpracy. Nowe Europejskie Centrum Doskonalenia w dziedzinie zwalczania zagrożeń hybrydowych w stolicy Finlandii Helsinkach odgrywa wyjątkową rolę w usprawnianiu tej współpracy[30]. W 2016 roku Komisja Europejska i Europejska Służba Działań Zewnętrznych wypracowały wspólne ramy dotyczące zwalczania zagrożeń hybrydowych, zawierające 22 działania, które mają być podjęte przez państwa członkowskie Unii oraz instytucje w celu rozpoznania zagrożeń hybrydowych, podniesienia świadomości tych zagrożeń, a także podjęcia kroków w kierunku budowania odporności. Chociaż działania te w żadnej mierze nie wyczerpują tego zagadnienia, wspólne ramy określiły jednoznaczną ambicję, aby zwalczanie zagrożeń hybrydowych stało się priorytetem Unii Europejskiej. Najbardziej konkretne efekty to utworzenie Komórki UE ds. syntezy informacji o zagrożeniach hybrydowych w ramach Centrum Wywiadowczego i Sytuacyjnego UE, a także Europejskiego Centrum Doskonalenia w dziedzinie zwalczania zagrożeń hybrydowych w Helsinkach. Zagrożenia hybrydowe awansowały również do rangi głównych priorytetów NATO, które przyjęło strategię zwalczania zagrożeń hybrydowych opartą na horyzontalnym podejściu.

Podobnie jak Unia Europejska, NATO stworzyło zaplecze do monitorowania i analizowania zagrożeń hybrydowych, oparte na społeczności wywiadowczej i współpracujące z innymi organami NATO. NATO stworzyło zespoły wspomagające ds. zwalczania zagrożeń hybrydowych, które mogą być wysyłane do wspierania władz w państwie dotkniętym takimi zagrożeniami. Komisja Europejska i Europejska Służba Działań Zewnętrznych (ESDZ) stworzyły międzysektorową grupę

Arlington 2007; *idem*, *Hybrid Warfare…*; N.P. Freier, *Known Unknowns: Unconventional „Strategic Shocks" in Defense Strategy Development*, Carlisle 2008.

[29] P. Szymański, *op.cit.*

[30] A. Hagelstam, *Współpraca przeciwko zagrożeniom hybrydowym*, NATO, https://www.nato.int, 23.11.2018 (16.01.2021).

do zwalczania zagrożeń hybrydowych, która spotyka się regularnie na różnych szczeblach.

Jednym z najbardziej wymiernych rezultatów działań w dziedzinie zwalczania zagrożeń hybrydowych jest Centrum Doskonalenia Hybrid CoE w Helsinkach, które osiągnęło swój potencjał operacyjny we wrześniu 2017 roku[31]. Centrum Hybrid CoE organizuje regionalne seminaria w celu wymiany najlepszych praktyk w dziedzinie zwalczania zagrożeń hybrydowych w gronie państw nordyckich i bałtyckich, we współpracy z Dowództwem Sił Operacji Specjalnych NATO.

Zwalczanie zagrożeń hybrydowych jest jednym z najwyższych priorytetów dla NATO. Od przyjęcia strategii Sojuszu w odniesieniu do wojny hybrydowej w 2015 roku członkowie Sojuszu konsekwentnie poszerzają zasobność środków NATO do reagowania na wspomniane zagrożenia[32]. Stworzenie przez NATO Pionu Połączonego Wywiadu i Bezpieczeństwa w 2017 roku, obejmującego jednostkę specjalistycznie zajmującą się monitorowaniem i analizą zagrożeń hybrydowych, było ważnym krokiem umożliwiającym państwom członkowskim NATO lepsze łączenie faktów. W minionej dekadzie Rosja zastosowała pełen wachlarz zagrożeń hybrydowych skierowanych przeciwko zasobom, politykom i dostawom energetycznym członków NATO oraz innych państw.

Złośliwe cyberataki są jednym z elementów najczęściej stosowanych w kampaniach hybrydowych. Broń cyfrowa przez lata będzie pozostawać atrakcyjną opcją – może być stosowana przez państwa, ale także przez najemników i prywatne organizacje, bez ograniczeń geograficznych. Reagowanie na zagrożenia hybrydowe wymaga międzysektorowego podejścia. To skłoniło NATO do szukania innych opcji poza ustalonym formatem szczytów szefów pastw i rządów oraz spotkań ministrów spraw zagranicznych i obrony.

W maju 2019 roku nieformalne posiedzenie Rady Północnoatlantyckiej po raz pierwszy zgromadziło doradców ds. narodowego bezpieczeństwa oraz wysokich rangą wiodących krajowych specjalistów ds. zagrożeń hybrydowych[33]. Posiedzenie to uwypukliło znaczenie skupiania w jednym miejscu wiedzy eksperckiej w zakresie zagrożeń zarówno cywilnych, jak i wojskowych oraz wymiany doświadczeń poszczególnych państw odnośnie do radzenia sobie z wrogimi kampaniami hybrydowymi. Pokazało także wolę NATO, by realizować nowe i innowacyjne sposoby pokonywania zagrożeń hybrydowych.

[31] *Ibidem.*

[32] M. Ruhle, C. Roberts, *Zwiększanie zasobowości środków NATO do zwalczania zagrożeń hybrydowych,* NATO, https://www.nato.int, 19.03.2021 (16.01.2021).

[33] *Ibidem*.

W styczniu 2018 r. Komisja Europejska powołała grupę ekspertów wysokiego szczebla, która miała zaproponować działania mające na celu pomoc państwom członkowskim Unii oraz jej instytucjom zwalczać dezinformację i *fake news*. Grupa kierowana przez profesor Madeleine de Cock Buning w marcu 2018 roku opublikowała raport ze swoich prac, którego rekomendacje można podsumować w następujących punktach: 1) zwiększenie transparentności informacji publikowanych online, 2) promowanie edukacji z zakresu mediów oraz informacji, 3) wspieranie pozycji użytkowników oraz dziennikarzy przeciwko dezinformacji, 4) wspieranie różnorodności oraz samowystarczalności ekosystemu medialnego UE, 5) promowanie dalszych badań nad wpływem dezinformacji w Europie oraz stworzeniem odpowiednich narzędzi do przeciwdziałania *fake news*[34].

Unia Europejska definiuje dezinformację jako weryfikowalnie fałszywą lub mylącą informację tworzoną, przedstawianą i rozprzestrzenianą dla korzyści ekonomicznej bądź intencjonalnego zwodzenia opinii publicznej[35]. Dezinformacja znalazła się w polu uwagi instytucji unijnych głównie ze względu na potrzebę ochrony demokratycznych procesów wyborczych przed ingerencją i manipulacjami zewnętrznych aktorów oraz na działalność organizacji terrorystycznych. Głównymi zadaniami wspólnoty w tym obszarze są monitorowanie i ujawnianie kampanii dezinformacyjnych i współpraca z platformami internetowymi[36].

W Polsce działania w obszarze przeciwdziałania dezinformacji prowadzone są m.in. przez Biuro Bezpieczeństwa Narodowego. Zdaniem BBN odpowiedź na dezinformację powinna mieć charakter systemowy, a zarządzanie systemem komunikacji powinno odbywać się na poziomie strategicznym. Dlatego system komunikacji strategicznej i przeciwdziałania dezinformacji powinien obejmować następujące obszary: koordynację komunikacji strategicznej; aktywne przeciwstawianie się dezinformacji (monitoring, analiza i kształtowanie polskiej przestrzeni informacyjnej, angażowanie obywateli, mediów, platform internetowych, organizacji pozarządowych); zwiększenie świadomości społecznej (szkolenia, edukacja medialna na wszelkich poziomach nauczania); aktywna obrona cyberprzestrzeni (monitorowanie i reagowanie na zagrożenia w Polsce i poza granicami przez placówki dyplomatyczne i siły zbrojne); polski *soft power* (budowanie kanałów komunikacji wykorzy-

[34] P. Chomicka, *Unia Europejska versus Dezinformacja – syzyfowa praca?*, Fundacja im. Kazimierza Pułaskiego, https://pulaski.pl, 23.03.2021 (26.01.2023).

[35] *Tackling online disinformation*, European Commission, https://ec.europa.eu, 15.01.2023 (21.02.2023).

[36] P. Szymański, *op.cit.*

stujących kulturę masową, długofalowe działania zmierzające do kreowania pozytywnego wizerunku na świecie i uniemożliwiających prowadzenie kampanii dezinformacyjnych wymierzonych w Polskę)[37].

Zakończenie

Nowe wyzwania stawiają szczególne wymagania wobec teorii i praktyki kształtowania systemu bezpieczeństwa informacyjnego państwa. Trudność w poszukiwaniu rozwiązań w tym zakresie polega na konieczności jednoczesnego rozpatrywania wielu składowych podejmowanych działań społecznych, gospodarczych, politycznych i militarnych kierowanych interesem narodowym; ich wpływu na stan bezpieczeństwa państwa i uwzględniania wyzwań zmieniającej się rzeczywistości. Wśród wielu rozpatrywanych czynników gwałtowny rozwój technologii informacyjnych i wynikające z tego konsekwencje wymagają szczególnej uwagi, gdyż stanowią istotny obszar uwarunkowań, od których zależą możliwości kształtowania bezpieczeństwa narodowego. Przekonanie o zasadności tego stwierdzenia wynika chociażby z pobieżnej analizy obserwowanych kierunków rozwoju techniki teleinformatycznej i mediów, wyznaczających przyszłe zmiany struktury systemu społecznego działania.

Jednak niekwestionowany pozostaje fakt, że w dobie społeczeństwa informacyjnego rozwój teleinformatyki, a szczególnie infrastruktury telekomunikacyjnej powoduje określone skutki – zmiany w strukturach działania narodu, które pośrednio lub bezpośrednio wpływają na bezpieczeństwo informacyjne państwa, gdyż przez szeroką wymianę informacji mają możliwości wrogich działań, tworząc zagrożenia jego ekonomicznego bezpieczeństwa, oraz decydują o wielkości zasobów, jakimi może dysponować naród, aby przeciwstawić się temu niebezpieczeństwu.

Zagrożenia hybrydowe są różnorodne i ciągle się zmieniają, a narzędzia sięgają w pełnym spektrum od fałszywych profili w mediach społecznościowych, przez zaawansowane ataki cybernetyczne, aż po otwarte użycie siły zbrojnej. Hybrydowe narzędzia wywierania wpływu mogą być stosowane oddzielnie lub w połączeniu, w zależności od celu i oczekiwanych rezultatów. Zagrożenia hybrydowe bezpieczeństwa informacyjnego państwa są zagrożeniami realnymi wpływającymi na funkcjonowanie społeczeństw, dlatego zwalczanie tych zagrożeń musi być dynamiczne i elastyczne.

[37] *Raport. Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo, społeczeństwo, polityka, biznes*, red. M. Wrzosek, Warszawa 2019, s. 9–10.

Bibliografia

Barć M., *Planning and Organising Protection of Critical Infrastructure,* „Polityka i Społeczeństwo", 2022, nr 2.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006.

Bednarski M.J., *Policja a środki masowego przekazu. Wybrane aspekty prawne*, Warszawa 2013.

Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia, red. S. Sulowski, M. Brzeziński, Warszawa 2009.

Borkowski R., *Fabryki strachu – obraz terroryzmu jako kicz w medialnej popkulturze. Zagrożenia bezpieczeństwa międzynarodowego* [w:] *Analiza informacji. Teoria i praktyka*, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2012.

Chomicka P., *Unia Europejska versus Dezinformacja – syzyfowa praca?*, Fundacja im. Kazimierza Pułaskiego, https://pulaski.pl, 23.03.2021 (26.01.2023).

Ciekanowski Z., Nowicka J., Wyrębek H., *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń,* Siedlce 2017.

Fake news – dezinformacja online, Warszawa 2020.

Freier N.P., *Known Unknowns: Unconventional „Strategic Shocks" in Defense Strategy Development*, Carlisle 2008.

Golka M., *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Warszawa 2008.

Górka M., *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa* [w:] *Cyberbezpieczeństwo wyzwaniem XXI wieku*, red. T.R. Dębowski, Wrocław 2018.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* „Bezpieczeństwo Narodowe", 2012, nr 22.

Hagelstam A., *Współpraca przeciwko zagrożeniom hybrydowym*, NATO, https://www.nato.int, 23.11.2018 (16.01.2021).

Hoffman F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007.

Hoffman F.G., *Hybrid Warfare and Challenges*, „Joint Force Quarterly", 2009, nr 52.

Jurgilewicz M., *Rola terenowych organów administracji publicznej w zapewnianiu bezpieczeństwa i porządku publicznego*, Warszawa 2023.

Kijewski T., *Znaczenie zagrożeń hybrydowych dla bezpieczeństwa Polski i państw NATO,* The Warsaw Institute Review, https://warsawinstitute.org, 16.02.2023 (20.02.2023).

Krzak A., *Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego,* „Przegląd Bezpieczeństwa Wewnętrznego", 2018, nr 18.

Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017.

Mockaitis T.R., *British Counterinsurgency in the Post-imperial Era*, London 1995.

Michalski K., Jurgilewicz M., *Konflikty technologiczne. Nowa architektura zagrożeń w epoce wielkich wyzwań*, Warszawa 2022.

Nemeth W.J., *Future war and Chechnya: A case for hybrid warfare*, Monterey 2002, Calhoun: Naval Postgraduate School, http://calhoun.nps.edu, 1.06.2002 (5.02.2023).

Newman N.J., *Asymmetric Threats to British Military Intervention Operations*, London 2000.

Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.

Nowicka J., Elak H., Ciekanowski Z., *Bezpieczeństwo jako kategoria funkcjonowania państwa* [w:] *Współczesne zagrożenia bezpieczeństwa państwa*, red. Z. Ciekanowski, cz. II, Biała Podlaska 2021.

Potejko P., *Bezpieczeństwo informacyjne* [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Warszawa 2009.
Projekt Doktryny bezpieczeństwa informacyjnego RP, BBN 2015.
Raport: Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo, społeczeństwo, polityka, biznes, red. M. Wrzosek, Warszawa 2019.
Ruhle M., Roberts C., *Zwiększanie zasobowości środków NATO do zwalczania zagrożeń hybrydowych*, NATO, https://www.nato.int, 19.03.2021 (16.01.2021).
Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia,* „Przegląd Bezpieczeństwa Wewnętrznego", 2016, nr 14.
Sun Tzu, *Sztuka wojny*, Warszawa 2021.
Supel A. [i in.], *Edukacja i wychowanie na rzecz bezpieczeństwa i obronności – wybrane aspekty*, „Polityka i Społeczeństwo", 2022, nr 3.
Szymański P., *NATO i Unia Europejska wobec zagrożeń hybrydowych,* Ośrodek Studiów Wschodnich, https://www.osw.waw.pl, 24.04.2020 (20.02.2023).
Tackling online disinformation, European Commission, https://ec.europa.eu, 15.01.2023 (21.02.2023).
Więcaszek-Kuczyńska L., *Zagrożenia bezpieczeństwa informacyjnego*, „Obronność. Zeszyty Naukowe", 2014, nr 2.
Wyrębek H., *Cyberprzestrzeń. Zagrożenia. Strategie bezpieczeństwa,* Siedlce 2021.
Wyrębek H., *National security challenges and threats*, „Wiedza Obronna", 2022, nr 2.
Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki Kolegium Analiz Ekonomicznych", 2013, nr 29.

Hybrid threats to state information security

Abstract

The annexation of Crimea and the beginnings of Russian aggression in the Donbass area have sparked widespread use in journalistic discourse and scholarly considerations of the concept of hybrid threats. With threats such as spreading false information and manipulating it in a way that undermines the public's trust in government and spreading information that compromises politicians. By attempting to undermine the social contract that binds the state and its constituents, a hybrid actor seeks to undermine trust between state institutions and citizens. As a result, the state loses its legitimacy - which is largely a function of public trust - and thus loses its ability to act as Thomas Hobbes argued in his 1651 work Leviathan. Consequently, a group of hybrid threats pertaining to information activities destroys both the ideological foundations and the state's ability to function smoothly. The article attempts to analyze and assess the essence of hybrid threats that have a major impact on the reduction of the state's information security.

Keywords: disinformation, countering disinformation, fake news, deepfake, hybrid attacks, hybrid warfare