SPRAWY MIĘDZYNARODOWE

2022, t. 75, nr 2
ISSN 0038-853X
e-ISSN 2720-0361
DOI 10.35757/SM.2022.75.2.03

Dezinformacja i operacje wpływu

ROBERT KUPIECKI
Uniwersytet Warszawski, Wydział Nauk Politycznych i Studiów Międzynarodowych
ORCID: 0000-0003-3419-6948
r.kupiecki@uw.edu.pl

NATO a dezinformacja
Siedem dekad doświadczeń

NATO's seventy years war against disinformation

Słowa kluczowe:
NATO, Rosja, dezinformacja, zagrożenia hybrydowe, odporność

Keywords:
NATO, Russia, disinformation, hybrid threats, resilience

NATO a dezinformacja. Siedem dekad doświadczeń

Rosyjska dezinformacja wymierzona w NATO poprzedza powstanie tej organizacji w 1949 r. Przez ponad siedemdziesiąt lat istnienia Sojuszu kampanie informacyjne Moskwy były konsekwentnie kierowane przeciwko spójności NATO, bezpieczeństwu politycznemu państw demokratycznych, społeczeństwu obywatelskiemu oraz wolności wyboru opartej na wiedzy i zaufaniu publicznym, a w kategoriach wojskowych – przeciwko wiarygodnemu odstraszaniu i kolektywnej obronie. Dezinformację traktowano jako substytut gorącego konfliktu i asymetryczną taktykę wzmacniania wpływu innych sposobów rywalizacji z Zachodem. Kolejne dekady potwierdziły ciągłość rosyjskich celów strategicznych i miejsce aktywnych działań w arsenale Moskwy. Lata te ukształtowały również *modus operandi* strategicznej komunikacji NATO, opartej na zweryfikowanych, prawdziwych i aktualnych informacjach. Obecnie masowość, szybkość i nowoczesne technologie w służbie rosyjskiej dezinformacji (i w coraz większym stopniu chińskiej) spowodowały intensyfikację działań NATO w tym obszarze. Postrzeganie zagrożenia dezinformacją jako autonomicznego wyzwania i elementu złożonych scenariuszy hybrydowych realizowanych przez zachodnich adwersarzy podkreślane jest od czasu nielegalnej aneksji Krymu przez Rosję w 2014 r. w dokumentach strategicznych NATO, w tym w najnowszej edycji koncepcji strategicznej (2022).

NATO's seventy years war against disinformation

Russian disinformation directed against NATO predates the organisation's birth in 1949. For more than 70 years of the alliance's existence, Moscow's information operations have been consistently directed against NATO's cohesion, the political security of democratic states, civil society and freedom of choice based on knowledge and public trust, and in military terms, against credible deterrence and collective defence. Disinformation was treated as a substitute for a hot conflict and as an asymmetric tactic to reinforce the impact of other means of rivalry with the West. The next few decades confirmed the continuity of Russian strategic goals and the place of active measures in Moscow's arsenal. Those years have also shaped the modus operandi of NATO's strategic communications based on verified, truthful and timely information. Nowadays, the massive scale, speed and modern technologies in the service of Russian (and increasingly Chinese) disinformation brought about an intensification of NATO's activities in this area. The perception of the threat posed by disinformation as an autonomous challenge, and a component of complex hybrid scenarios pursued by Western adversaries, has been emphasised, since Russia's illegal annexation of Crimea in 2014, by NATO's strategic documents, including the latest edition of its Strategic Concept (2022).

NATO konfrontuje się z dezinformacją od swojego powstania w 1949 r., choć w istocie sowieckie działania propagandowe mające zohydzać w oczach światowej opinii publicznej sojusz państw zachodnich (jako narzędzie agresji, prowokację amerykańskiego imperializmu i wroga ludzkości) poprzedzały moment podpisania *Traktatu północnoatlantyckiego*. W kolejnych latach konsekwentnie stosowano je przeciwko bezpieczeństwu politycznemu państw zachodnich, społeczeństwu obywatelskiemu i wolności wyboru opartej na wiedzy i zaufaniu społecznym, a w sensie militarnym – przeciwko wiarygodnemu odstraszaniu i kolektywnej obronie sojuszniczej[1]. Dobrze zbadanymi przykładami takich kampanii propagandowych Związku Sowieckiego przeciwko Zachodowi i NATO są m.in. operacje dezinformacyjne dotyczące mostu powietrznego USA ustanowionego w odpowiedzi na sowiecką blokadę Berlina Zachodniego w latach 1948–1949, dezinformacja na temat wojny w Korei (1950–1953) czy wielokierunkowe działania dezinformacyjne dotyczące tzw. *dual-track decision* NATO, związanej z rozmieszczeniem w Europie pocisków nuklearnych pośredniego zasięgu (INF)[2].

W każdym z tych przypadków dezinformacja traktowana była jako substytut gorącego konfliktu i asymetryczna taktyka wzmacniająca oddziaływanie innych środków zimnowojennej rywalizacji. W ostatecznym rozrachunku osłabianie morale zachodnich społeczeństw i ośrodków władzy państwowej miało przygotowywać korzystniejszy grunt na wypadek czynnego konfliktu militarnego. Stosowanie dezinformacji było tańsze niż tradycyjne narzędzia przymusu wykorzystujące potęgę państwa i łatwiejsze do ukrycia. Pozwalało wypierać się sprawstwa, a jednocześnie zachowywać inicjatywę strategiczną, podczas gdy działania broniącej się strony były spóźnione i nieadekwatne do szybko

1 K. Giles, A. Seaboyer, *The Russian information warfare construct*, Royal Military College, Kingston, March 2019: <https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf> [dostęp: 22 VII 2022].

2 Szczególnie ta ostatnia kampania jest dobrze zbadana źródłowo. Zob. m.in.: C. A. Sorrels, *Soviet propaganda campaign against NATO*, US Arms Control and Disarmament Agency, Washington DC, October 1983: <www.insidethecoldwar.org/sites/default/files/documents/Soviet%20Propaganda%20Campaign%20Against%20NATO_0.pdf> [dostęp: 21 VII 2022]; R. Kupiecki, *Siła i solidarność. Strategia NATO 1949–1989*, Polski Instytut Spraw Międzynarodowych, Warszawa 2012, s. 290–300.

rozprzestrzeniającego się fałszu – współcześnie korzystającego z technologii przyspieszających i decentralizujących przekaz informacji.

Sowiecki *modus operandi* w zakresie dezinformacji opierał się m.in. na odwracaniu znaczeń słów, przypisywaniu agresywnych intencji przeciwnikowi, straszeniu wojną, masowym wprowadzaniu do obiegu publicznego fałszywych informacji, pogłębianiu naturalnych różnic opinii występujących w społeczeństwach demokratycznych czy wykorzystywaniu organizacji społeczeństwa obywatelskiego i własnej agentury na Zachodzie do ideologicznej dywersji. W kolejnych antynatowskich (i szerzej: antyzachodnich oraz antyamerykańskich) kampaniach Sowieci wykorzystywali wspomniane techniki w zmieniających się kontekstach sytuacyjnych, ale wykazywali także zdolność uczenia się i stosowania najnowszych zdobyczy technologicznych, a także wiedzy o psychologii, procesach poznawczych oraz komunikacji jednostek i zbiorowości. Po zakończeniu zimnej wojny model ten zasadniczo przejęła do swoich antynatowskich kampanii Rosja[3]. Zmieniła się jednak ich natura – zamiast poszczególnych akcji mamy bowiem ciągłość agresywnych działań informacyjnych, a nowoczesne technologie informacyjne pozwalają na zwiększenie ich skali i tym samym zwielokrotnienie zagrożeń dla państw NATO. Obok Rosji jako nowy aktor antyzachodniej dezinformacji coraz silniej dają o sobie znać Chiny[4]. Zagrożenie to skupia uwagę cywilnych i wojskowych władz NATO oraz jego państw członkowskich. Pozostaje jednak pytanie: czy podejmowane przez nie kroki skrojone są na miarę szkodliwego potencjału dezinformacji i ewentualnie od kiedy?

3 Znalazł on też miejsce w rosyjskich doktrynach wojskowych z XXI w. oraz rozważaniach doktrynalnych, zwłaszcza upublicznionych przez szefa sztabu generalnego Walerija Gierasimowa, który głosi zmianę charakteru wojen i wzrost roli środków niemilitarnych w osiąganiu celów politycznych i strategicznych. Zob. M. Galeotti, *The mythical „Gerasimov Doctrine" and the language of threat*, „Critical Studies on Security" 2019, vol. 7, No. 2, DOI: 10.1080/21624887.2018.1441623, s. 157–161; L. Kucharski, *Russian multi-domain strategy against NATO: Information, confrontation and US forward-deployed nuclear weapons in Europe*, U.S. Department of Energy, Office of Scientific and Technical Information, 2018, DOI: 10.2172/1635758: <www.osti.gov/servlets/purl/1635758> [dostęp: 4 VII 2022].

4 Analiza różnic w operacyjnych modelach rosyjskiej i chińskiej dezinformacji: R. Kupiecki, F. Bryjka, T. Chłoń, *Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przeciwdziałanie*, Wydawnictwo Naukowe „Scholar", Warszawa 2022, s. 94–97.

Rosyjska dezinformacja przeciwko NATO – ciągłość i zmiana

Natura problemu zwalczania dezinformacji w działaniach NATO – pomimo istotnych zmian w charakterystyce zagrożenia, które wynikają z ewolucji kontekstu strategicznego i możliwości stwarzanych przez postęp technologiczny w sferze informacyjnej – wykazuje wiele cech ciągłości. Stanowią o tym cztery zasadnicze kwestie: trzy z nich dotyczą charakterystyki działań rosyjskich, a jedna – podejścia sojuszniczego:

– źródło i dysponent dezinformacji skierowanej przeciwko NATO oraz jego cele,

– ogólne techniki wykorzystywane w prowadzonych przez niego operacjach informacyjnych,

– strategiczne ulokowanie dezinformacji jako narzędzia jego polityki zagranicznej i bezpieczeństwa oraz utrzymanie przez państwo kontroli nad operatorami i treścią takich działań,

– długotrwałe i zasadniczo błędne odczytywanie w NATO sowieckiej i następnie rosyjskiej dezinformacji jako taktyki wzmacniającej jedynie wojskowe plany Moskwy, a nie zagrożenia *per se*.

1. Źródłem zagrożeń dla NATO jest niezmiennie polityka Moskwy, która zarówno w czasach sowieckich, jak i obecnie postrzega istnienie i rozwój sojuszu państw zachodnich oraz wojskową obecność USA w Europie jako przeszkodę w realizacji swoich celów geopolitycznych. W węższym rozumieniu jednak, poprzez środki aktywne – osłabianie zdolności poznawczych przeciwnika i wpływanie na jego procesy decyzyjne – dezinformacja stanowi taktykę wspierającą osiąganie celów Kremla[5]. Od lat dwudziestych XX w. doświadczenia tajnej policji carskiej systematycznie i w oparciu o wiedzę naukową rozwijane były i doskonalone przez Związek Sowiecki jako narzędzie działań skrytych, przenikających tradycyjne sektory bezpieczeństwa[6]

5 Zob. D. Kux, *Soviet active measures and disinformation. Overview and assessment*, „Parameters" 1985, No. 4, s. 19–28; *Active measures: A report on the substance and process of anti-U.S. disinformation and propaganda campaigns*, US State Department, August 1986: <www.insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20Substance%20and%20Process%20of%20Anti US%20Disinformation%20August%201986.pdf> [dostęp: 1 VII 2022]; M. Wojnowski, *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 11–36.

6 Polityczne, wojskowe, gospodarcze, społeczne i środowiskowe.

oraz jego wymiary wewnętrzny i międzynarodowy[7]. Wobec NATO i jego państw członkowskich dezinformacja wykorzystywana była celem rozbicia współpracy sojuszników, wzmocnienia polaryzacji ich stanowisk w sprawach międzynarodowych i wypchnięcia z Europy USA jako czynnego gwaranta bezpieczeństwa militarnego Zachodu, co miało prowadzić do rozkładu kolektywnej obrony i osłabienia wewnętrznej spójności zachodnich demokracji, a w ślad za tym do zwiększenia inicjatywy i sprawczości Rosji w polityce międzynarodowej. Podważenie spójności NATO, obok zmiany równowagi wojskowej na świecie, powodowałoby bowiem, że Moskwa nie musiałaby się konfrontować ze skoordynowanym stanowiskiem Zachodu. To z kolei prowadziłoby do nieuchronnej bilateralizacji jej stosunków z państwami zachodnimi, pozwalającej korzystać ze źródeł własnych przewag oraz rozgrywać podziały międzynarodowe i wewnątrzpaństwowe.

2. Jeśli idzie o tradycyjne techniki rosyjskiej dezinformacji wykorzystywane przeciwko NATO i jego państwom członkowskim, badacze wskazują na ich zasadniczą ciągłość i osadzenie w tradycji[8]. Ustalenia w tej mierze wiele zawdzięczają Benowi Nimmo, który powtarzające się sposoby działania rosyjskich dezinformatorów państwowych na tym polu scharakteryzował jako 4D:

– odrzucenie krytyki (*dismiss*) – polegające na aktywnym zaprzeczaniu jej lub piętnowaniu krytyków Rosji (działającej jakoby zawsze słusznie) jako nieobiektywnych, źle poinformowanych lub kierujących się niskimi pobudkami;

7 Istnieje bogata literatura przedmiotu omawiająca genezę tego zjawiska. Zob. m.in.: I. M. Pacepa, J. R. Rychlak, *Dezinformacja: były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu*, przeł. M. Machnik, Editio, Gliwice 2015; T. Rid, *Wojna informacyjna*, przeł. M. Tyl, Bellona, Warszawa 2020; K. Giles, *Handbook of Russian information warfare*, NATO Defence College, Rome 2016 (Fellowship Monograph, 9): <www.researchgate.net/publication/313423985_Handbook_of_Russian_Information_Warfare> [dostęp: 11 IV 2022]; M. Galeotti, *Russian political war. Moving beyond the hybrid*, Routlegde, London–New York 2019; R. Kupiecki, F. Bryjka, T. Chłoń, *Dezinformacja…*; V. Volkoff, *Dezinformacja. Oręż wojny*, przeł. A. Arciuch, Delikon, Warszawa 1991; tenże, *Petite histoire de la désinformation. Du cheval de troie à internet, le rocher*, Éditions du Rocher, Paris 1999.

8 Brytyjski analityk Andrew Wilson osadza je w tradycji sowieckiej. Zob. A. Wilson, *Four types of Russian propaganda*, „Aspen Review" [online], 15 III 2017 [dostęp: 20 VII 2022]: <www.aspen.review/article/2017/four-types-of-russian-propaganda/>.

– wypaczanie faktów (*distort*) – będące w istocie odwracaniem narracji i znaczeń słów, obrazów oraz faktów (np. wydarzeń historycznych)[9] w luźnym związku z rzeczywistością lub nawet bez takowego. Obejmuje to również tworzenie alternatywnej rzeczywistości, opartej na tzw. wielkim kłamstwie, które w celu wykreowania nowego obrazu lub interpretacji pożądanej sprawy przekracza granice nie tylko prawdy, ale i zdrowego rozsądku;

– odwracanie uwagi od sedna sprawy (*distract*) – polegające na wprowadzaniu do debaty publicznej tematów zastępczych, promowaniu określonych fałszywych treści lub swoiście pojmowanego symetryzmu narracyjnego (od czasów rewolucji październikowej przeciwnikom Moskwy zarzuca się przewiny gorsze od tych, za które sama jest krytykowana);

– ogłupianie i zastraszanie odbiorców (*dismay*) – oparte na ciągłym wykazywaniu szkód, jakie zadają im krytycy Rosji, autowiktymizacji Rosji jako ofiary Zachodu i przedstawianiu własnej agresji jako działań motywowanych samoobroną[10].

Opisane przez Bena Nimmo narzędzia 4D kumulują się w odrębnej technice (swoistym piątym D)[11]. Można ją określić jako wprowadzanie u przeciwnika podziałów (*divide*) poprzez wykorzystywanie i pogłębianie naturalnych różnic opinii i postaw w demokratycznych społeczeństwach, podważanie autorytetów i wiedzy naukowej, masowe operowanie fałszywymi informacjami, co prowadzi do wzrostu podatności grup społecznych na zewnętrzne manipulacje. Co interesujące, dla rosyjskiej dezinformacji nie jest ograniczeniem ani prawda, ani zdrowy rozsądek, ani nawet ujawnienie fałszerstw – obwiązuje zasada ciągłości działań ofensywnych przy elastycznym dostosowywaniu do sytuacji fabuł narracyjnych[12].

9 Szerzej zob. *Disinformation, narratives and memory politics in Russia and Belarus*, ed. A. Legucka, R. Kupiecki, Routledge, London 2022.

10 B. Nimmo, *Anatomy of an info-war. How Russia's propaganda machine works and how to counter it*, „Stop Fake" [online], 19 V 2015 [dostęp: 22 VII 2022]: <www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it>.

11 Model ten wywodzi się z typologii narzędzi rosyjskiej dezinformacji opracowanej przez Bena Nimmo. Rozwijało go wielu badaczy, a jedna z najbardziej popularnych propozycji powstała pod auspicjami EU vs Disinfo. Zob. *Modus trollerandi*, p. 1–7, „EU vs Disinfo" [online, dostęp: 20 VII 2022]: <https://euvsdisinfo.eu/?s=modus+trollerandi>.

12 R. Kupiecki, *„Mit założycielski" polityki zagranicznej Rosji*, „Sprawy Międzynarodowe" 2019, t. 72, nr 4, DOI: 10.35757/SM.2019.72.4.03, s. 79–83.

3. O strategicznym ulokowaniu dezinformacji pośród arsenału środków aktywnych decyduje rozumienie jej przez Rosjan zarówno jako samodzielnego narzędzia, jak i składnika ciągłych wielopłaszczyznowych oddziaływań cywilno-wojskowych związanych ze strategicznymi celami państwa i wizją zagrożeń, pośród których czołowe miejsce zajmuje NATO[13]. Mogą być one prowadzone w czasach pokoju jako element polityki zagranicznej sprzyjający poprawie międzynarodowej pozycji państwa oraz ułatwiający działania wojskowe i wywiadowcze. Prowadzi to do zatarcia granic między ofensywną aktywnością polityczną a weaponizacją informacji jako składnikiem niekończącej się wojny politycznej (czyli szczególnych operacji w czasach pokoju, pokrewnych działaniom wojskowym) lub zupełnie do zniknięcia w rosyjskiej myśli i praktyce strategicznej podziału na czas pokoju i wojny. Solidna analiza tej problematyki zawarta jest w publikacjach Marka Galeottiego[14].

4. Przez większość czasu po 1949 r. konfrontowane z dezinformacją Moskwy NATO postrzegało ją przede wszystkim jako zagrożenie integralnie zrośnięte z planowaniem wojskowym i pełniące rolę mnożnika siły. Nie było jednak traktowane jako samodzielny czynnik osłabiający sojuszniczy potencjał odstraszania i zdolności cywilno-wojskowe, a więc realizujący sowieckie lub rosyjskie cele niższym kosztem czy zgoła bez konieczności uciekania się do wojny[15]. W ostatniej dekadzie, a zwłaszcza po anektowaniu przez Rosję Krymu w 2014 r., rosnąca skala głównie rosyjskiej dezinformacji spowodowała rewizję tego podejścia. W sensie doktrynalnym jest ona obecnie traktowana jako składnik szerszego spektrum zagrożeń hybrydowych[16]. W warstwie

13 Percepcja NATO w rosyjskich dokumentach państwowych: *Documents talk. NATO–Russia relations after the Cold War*, ed. R. Kupiecki, M. Menkiszak, Polish Institute of International Affairs, Warsaw 2020.

14 M. Galeotti, *Controlling chaos. How Russia manages its political war in Europe*, European Council of Foreign Relations, 1 IX 2017: <www.ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/> [dostęp: 23 VI 2022]; tenże, *Russian…*; tenże, *The „Gerasimov Doctrine" and Russian non-linear war*, „In Moscow's Shadows" [online], 7 X 2015 [dostęp: 14 VI 2022]: <www.inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>.

15 K. Giles, *Handbook…*, s. 16–27.

16 *NATO's response to hybrid threats*, „North Atlantic Treaty Organization" [online], 21 VI 2022 [dostęp: 25 VII 2022]: <www.nato.int/cps/en/natohq/topics_156338.htm>;

operacyjnej zwalczanie dezinformacji jako samodzielnego zagrożenia przykuwa coraz większą uwagę organów NATO. Obejmuje to m.in. wysiłki na rzecz wzmocnienia koordynacji działań z sojusznikami i państwami partnerskimi, a także podniesienie ich standardu opartego na przekazie wiarygodnych i zweryfikowanych informacji oraz rozwoju systemowej odporności społecznej na tego rodzaju zagrożenia.

Podejście NATO do zwalczania dezinformacji w latach zimnej wojny

W czasie zimnej wojny Sojusz Północnoatlantycki umieszczał możliwe skutki wrogiej propagandy i dezinformacji we własnej ocenie zagrożeń. Znajdowało to odzwierciedlenie nie tylko w stopniowym rozwoju aktywnej komunikacji strategicznej kształtującej wizerunek NATO, lecz również w udostępnianiu wiedzy na jego temat międzynarodowej opinii publicznej. Problematyka ta ujmowana była również w niejawnych dokumentach organizacji dotyczących procesu planowania obronnego. Chodzi tu zwłaszcza o trzy zimnowojenne koncepcje strategiczne i związane z nimi wytyczne dla kolektywnej obrony (zawarte w dokumentach serii MC-400)[17].

Już pierwsza strategia NATO z 1949 r. (DC 6/1)[18] zwracała uwagę na potrzebę wymiany informacji o zagrożeniach oraz współpracy państw członkowskich w obronie przed wojną psychologiczną i operacjami specjalnymi, a także przygotowywania własnych. W wypracowanych na tej podstawie w 1950 r. *Strategicznych zaleceniach w sprawie planowania regionalnego NATO* (MC 14) przygotowania obronne w tej dziedzinie ujmowano pod ogólną kategorią „przeciwdziałania aktom dywersji na obszarze północnoatlantyckim". Ten kierunek planowania wojskowego NATO znajdował oparcie w analizach politycznych, które zwracały uwagę na specyficzną cechę sowieckiej strategii. W korespondencji dyplomatycznej z 1952 r. ówczesny ambasador USA w Moskwie George F. Kennan wskazywał na unikanie przez

B. Najzer, *The hybrid age. International security in the era of hybrid warfare*, Bloomsbury Publishing, London 2020.

17 Ich oryginalny zbiór: *NATO strategy documents 1949–1969*, ed. G. D. Pedlow, Historical Office SHAPE, NATO International Staff Central Archives, Brussels 1997.

18 Tłumaczenia zimnowojennych koncepcji strategicznych NATO: R. Kupiecki, *Siła…*, s. 396–435.

Sowietów otwartej konfrontacji wojskowej z Zachodem i skłonność do agresji środkami pośrednimi, takimi jak kłamstwo, dywersja, wojna psychologiczna i brutalne wykorzystywanie wszelkich różnic występujących w polityce wewnętrznej państw zachodnich oraz między nimi na arenie międzynarodowej. Agresywne zachowania, których zestaw sporządzony został na podstawie analizy polityki bloku sowieckiego, interpretowano przy tym bardzo szeroko – od tajnych operacji i dywersji aż po agresję zbrojną oraz maskowanie swych intencji „gestami dobrej woli oraz ofertami pomocy politycznej, gospodarczej i wojskowej"[19].

W podobny sposób stanowisko NATO przedstawione zostało w strategii zmasowanego odwetu z 1957 r. (MC 14/2). Uwagę zwraca tu integralne podejście do zagrożeń i ich geograficznego występowania[20], zdefiniowanych szeroko – od dywersji, sabotażu i wrogiej infiltracji po wojnę nuklearną. Pośród środków stosowanych przez Sowietów celem „objęcia całego świata wpływem komunizmu we własnej wersji" wskazane zostały m.in. instrumenty polityczne i gospodarcze, tajne operacje[21], propaganda i dywersja (w tym szerzenie ideologii komunistycznej i wywoływanie niepokojów) oraz destabilizacja wrażliwych miejsc na świecie. Chociaż zagrożenie zostało określone jako globalne, to jednak w strategii NATO zwrócono uwagę na ostrożność działań Moskwy w Europie. Sojusz oceniał je jako nakierowane na rozproszenie sił, podważenie spójności, osłabienie woli i zdolności do prowadzenia kolektywnej obrony oraz przygotowanie gruntu pod przyszłą agresję. Jasno też pojmowano, że mogą być one nasilane, jeśli przeciwnik dostrzeże brak determinacji Zachodu do przeciwdziałania, co w konsekwencji może doprowadzić do ograniczonej agresji militarnej.

Pogłębienie tej refleksji znalazło się w ostatniej natowskiej strategii z lat zimnej wojny, czyli strategii elastycznego reagowania z 1967 r.

19 *Foreign Service Dispatch 116 of September 8, 1952, US Embassy Moscow, The Soviet Union and the Atlantic Pact*, [w:] G. F. Kennan, *Memoirs 1950–1963*, Little Brown, Boston 1971, s. 327–351.

20 Według dzisiejszej nomenklatury byłaby to wczesna edycja tzw. *360 degrees approach*.

21 Definiowane przez NATO jako każde działanie z pominięciem użycia broni jądrowej, które zostało zaplanowane i wykonane w sposób umożliwiający ukrycie tożsamości lub wyparcie się przez organizatora związku z takim działaniem.

(MC 14/3). Zasadniczy kierunek oceny omawianych zagrożeń nie uległ tam zmianie. Wyraźnie zaktualizowano jednak analizę sposobu operowania Sowietów, akcentując np. korzystanie przez nich w działaniach dywersyjnych z lokalnych aktorów zastępczych[22] w postaci użytecznych idiotów czy ideologicznie motywowanych grup reprezentujących społeczeństwo obywatelskie.

W czasie zimnej wojny w NATO nie tylko dostrzegany był więc problem, ale też widać było poprawne rozumienie zagrożenia wynikającego z wrogich oddziaływań informacyjno-psychologicznych. W ślad za tym analizowano sytuację i aktualizowano stosowną wiedzę oraz właściwie rozpoznawano ich ogólną naturę. Przeciwdziałanie tym zagrożeniom postrzegane było także jako integralny składnik przygotowań obronnych oraz polityki odstraszania. W tym miejscu przejawiały się jednak istotne ograniczenia sojuszniczej analizy sowieckiej dezinformacji i w istocie horyzontów wyobraźni strategicznej. Dotyczyły one przede wszystkim braku zrozumienia dla autonomii tego środka walki, postrzeganego wyłącznie jako składnik szerszego zestawu narzędzi ofensywnych, a w najlepszym wypadku – ich wzmacniacz, ściśle związany ze scenariuszami wojskowymi. Trudno więc wskazać na zestaw odpowiedzi NATO, które byłyby adekwatne do strategicznej natury zagrożenia oraz instrumentalizowania go w polityce zagranicznej przeciwnika. Bardziej niż w oparciu o stałe procedury reagowania na dezinformację sojusz skłonny był tu działać reaktywnie lub polegać na sile swoich wolnych instytucji i edukacji społecznej.

Stopniowo jednak NATO zwiększało systematyczność swoich działań, koncentrując się na:

– rozpoznawaniu dezinformacji skierowanej przeciwko sojuszowi,

– wypracowaniu zdolności odpowiadania na wrogie operacje informacyjne,

– ochronie własnego przekazu publicznego związanego z misją i polityką NATO jako sojuszu obronnego i wspólnoty wartości,

– wzmacnianiu spójności członków organizacji i ich odporności na wrogą dezinformację,

22 Szeroka analiza zjawiska: F. Bryjka, *Wojny zastępcze*, Polski Instytut Spraw Międzynarodowych, Warszawa 2021.

– poszerzaniu wiedzy państw członkowskich na temat antynatowskiej dezinformacji i w miarę możliwości wspieraniu ich w rozwoju zdolności do przeciwdziałania temu zagrożeniu.

Trudno było jednak mówić o specyficznym *modus operandi* sojuszu w tym zakresie, choć niewątpliwie zebrał on niemałą wiedzę na temat tego rodzaju zagrożeń, które w pozimnowojennych dekadach ujawniły się z nową siłą. Niezależnie od refleksji NATO w tym względzie lwią część odpowiedzialności za walkę z dezinformacją ponosiły po prostu państwa członkowskie.

Déjà vu? NATO a rosyjska dezinformacja po zakończeniu zimnej wojny

Po zakończeniu zimnej wojny rosyjskie cele strategiczne wobec wspólnoty zachodniej, których osiąganiu ma służyć dezinformacja, zasadniczo się nie zmieniły. Wzrosła jednak liczba aktów agresji informacyjnej przeciwko NATO oraz ich złożoność, a także spektrum wykorzystywanych w tym celu środków (ludzkich i technicznych)[23]. Rewolucja technologiczna, a zwłaszcza internet i algorytmy wykorzystujące uczenie maszynowe, zmieniły charakter procesów komunikacyjnych, przyspieszając obieg informacji oraz zwiększając ich zasięg i liczbę. Dezinformacja w niezliczonych mutacjach narracyjnych, nowych postaciach (jak platformy cyfrowe i media społecznościowe) oraz maskach pojęciowych[24] zaczęła dotykać niemal każdej publicznej aktywności sojuszu. Celowo zniekształcona informacja skierowana przeciw NATO stała się także czynnikiem ułatwiającym wiązanie innych środków w hybrydowe scenariusze zagrożeń – nieograniczone w liczbie

23 Szerzej zob. A. Radin, A. Demus, K. Marcinek, *Understanding Russian subversion. Patterns, threat and responses*, RAND Corporation, 2020, DOI: 10.7249/PE331: <www.rand.org/pubs/perspectives/PE331.html> [dostęp: 19 VII 2022].

24 Np. klasyczna triada: dezinformacja (*disinformation*) – mylna informacja (*misinformation*) – szkodliwa informacja (*malinformation*), ale także propaganda (w odcieniach białym, szarym i czarnym), nie mówiąc już o rosyjskiej nomenklaturze (jak *środki aktywne*, *kontrola refleksywna/refleksyjna*, *wojna polityczna*, *operacje informacyjne*) itp. Objaśnienia tych pojęć i ich kontekstów operacyjnych: R. Kupiecki, F. Bryjka, T. Chłoń, *Dezinformacja…* Na stronach 161–185 wiele uwagi poświęcono tam organizacji i doktrynie rosyjskiej dezinformacji państwowej.

możliwych kombinacji i obszarów potencjalnych szkód (np. polityki, gospodarki[25], kultury i wiedzy naukowej, obronności czy cyberprzestrzeni).

Wykorzystują one chronioną prawem i obyczajem zachodnią przestrzeń wolności: słowa, wyborów, mediów, gospodarki i kultury debaty, które przez podmioty niezamierzające przestrzegać demokratycznych reguł gry politycznej traktowane są jako słabości[26]. W tych warunkach traktowana jako oręż dezinformacja zaburza relacje między elementami informacyjnego ekosystemu państw demokratycznych. Poprzez fałszowanie danych może wzbudzać niepokoje i nieufność wobec prawdy, podtrzymywać chaos, odwracać uwagę, wpływać na wyniki wyborów w innych państwach, pogłębiać podziały czy trwale zmieniać opinię społeczną wobec różnych spraw. W czasach pokoju może być prostszym, choć skutecznym środkiem oddziaływania na przeciwnika, tańszym i mniej kontrowersyjnym od środków przymusu politycznego, ekonomicznego lub otwartego konfliktu[27]. Intensywność i liczba operacji informacyjnych przeciwko NATO i jego państwom członkowskim wzrosła geometrycznie po anektowaniu przez Rosję Krymu w 2014 r. Ich wspólnymi cechami – jak słusznie wskazują analitycy RAND – stały się: mnogość oddziaływań, wykorzystywanie

25 W 2018 r. firma konsultingowa Prevency oszacowała, że światowa gospodarka corocznie traci wskutek dezinformacji 78 mld dol.: straty wizerunkowe – 17 mld, spadek wartości akcji – 39 mld, obniżenie reputacji firm – 10 mld i koszty prewencji (kampanii zwalczających dezinformację). Zob. *What is disinformation?*, „Prevency" [online, dostęp: 11 VII 2022]: <www.prevency.com/en/what-is-disinformation>.

26 Pracujący na zlecenie szwedzkiego resortu obrony zespół badawczy przypisuje rosnące znaczenie zagrożeń hybrydowych dla bezpieczeństwa Zachodu grupie sześciu czynników: rozpadowi liberalnego porządku międzynarodowego i przesuwaniu się osi konfliktów z tradycyjnych domen ku wpływaniu na zdolności poznawcze dużych grup społecznych; sieciowości powiązań międzynarodowych zaburzających tradycyjne postrzeganie potęgi; wpływom nowoczesnych technologii przenoszących konflikty poza tradycyjne i terytorialnie zdefiniowane obszary; przyspieszeniu obiegu informacji za sprawą internetu; ewolucji konfliktów i podniesieniu roli czynnika niemilitarnego; zmianom kulturowym rzucającym wyzwanie pamięci historycznej i fundamentom tożsamości narodów. Zob. G. Treverton i in., *Addressing hybrid threats*, Swedish Defense University, Stockholm 2018.

27 Choć sama skuteczność dezinformacji międzynarodowej jest dla jej badaczy kwestią sporną. Zob. m.in.: A. Lanoszka, *Disinformation in international politics*, „European Journal of International Security" 2019, vol. 4, issue 2, DOI: 10.1017/eis.209.6, s. 227–248; A. W. M. Gerrits, *Disinformation in international relations. How important is it?*, „Security and Human Rights" 2018, vol. 29, DOI: 10.1163/18750230-02901007, s. 3–23.

wielu kanałów przekazu, ciągłość, szybkość i powtarzalność działań, mała adekwatność narracji do obiektywnej rzeczywistości i brak respektu dla spójności przekazu[28]. Obiektami ataku stały się zaś m.in.:

– misje stabilizacyjne NATO w różnych miejscach świata,
– polityka wewnętrzna sojuszu (np. polityka otwartych drzwi),
– działania wzmacniające kolektywną obronę w różnych regionach obszaru północnoatlantyckiego,
– ćwiczenia wojskowe,
– intencje polityczne (np. wobec współpracy z Rosją) przedstawiane zgodnie z interpretacjami dezinformatorów,
– wysiłki na rzecz walki z pandemią COVID-19 i oparte na badaniach naukowych zalecenia medyczne (do tego doszły oskarżenia o wytworzenie koronawirusa w wojskowych laboratoriach NATO)[29],
– sojusznicze wsparcie dla zasad prawa międzynarodowego,
– wolne media w państwach członkowskich, autorytety społeczne czy kampanie wyborcze i referendalne (m.in. w USA, Francji, Niemczech i Wielkiej Brytanii).

Skala, intensywność oraz weaponizacja dezinformacji przez przeciwników NATO wymusiła usystematyzowanie podejścia do tego problemu w codziennej aktywności sojuszu. Niektórzy badacze mówią nawet o przyspieszonej sekurytyzacji[30], gdzie podmiotem sekurytyzującym jest NATO, odbiorcami – opinia publiczna państw członkowskich, żywotne zagrożenie płynie z Rosji, a chronionym dobrem jest spójność całej wspólnoty i jej bezpieczeństwo polityczno-militarne. Znakomitą analizę tego procesu, opartą na badaniach treści blisko 250 tys. oficjalnych przekazów NATO z lat 2014–2022, przynosi studium Akina Ünvera i Ahmeta Kurnaza. Autorzy ci pokazują m.in. ewolucję języka opisu zagrożeń, gdzie z sojuszniczego

28 Ch. Paul, M. Matthews, *The Russian „firehose of falsehood" propaganda model. Why it might work and options to counter it*, RAND Corporation, 2016, DOI: 10.7249/PE198: <www.rand.org/pubs/perspectives/PE198.html> [dostęp: 23 VII 2022].

29 Tu aktywne były również chińskie ośrodki dezinformacyjne.

30 M. Baumann, *Propaganda fights and disinformation campaigns: the discourse on information warfare in Russia-West relations*, „Contemporary Politics" 2020, vol. 26, No. 3, DOI: 10.1080/13569775.2020.1728612), s. 288–307. Wskazanie na owo przyspieszenie zasługuje na uwagę choćby z tego powodu, że dezinformacja nie była podejmowana w trzech kolejnych zapisach strategii NATO z lat 1991, 1999 i 2010. Zmiana w tej kwestii nastąpiła dopiero w 2022 r.

słownika politycznego dopiero około roku 2018 preferowany dotąd koncept działań hybrydowych wyparło bezpośrednie używanie pojęcia *dezinformacja* (oraz towarzyszących jej *misinformation*, *propaganda* i *fake news*)[31]. Przyjęta przez sojusz definicja operacyjna określa dezinformację jako „świadome tworzenie i rozprzestrzenianie fałszywych oraz zmanipulowanych informacji z zamiarem oszustwa lub wprowadzania w błąd, prowadzące do pogłębiania podziałów wśród sojuszników, co podrywa zaufanie obywateli do demokratycznie wybranych rządów"[32]. Tym samym jasno wskazano zarówno składniki i kryteria zagrożeń (świadomą i zamierzoną szkodliwość operacji informacyjnych), naturę problemu wymagającego kolektywnego działania sojuszników (polaryzację zachodnich społeczeństw), jak i zestaw wartości chronionych (demokrację i zaufanie społeczne).

Po anektowaniu Krymu przez Rosję skuteczna komunikacja strategiczna stała się jednym z priorytetów NATO, a po inwazji z lutego 2022 r. wzrosło jeszcze znaczenie przeciwdziałania dezinformacji, także jako wytyczna dla bieżącej aktywności Kwatery Głównej NATO. Na najwyższym szczeblu odnotowano to po raz pierwszy w deklaracji brukselskiego szczytu sojuszu z 2018 r. Szefowie państw i rządów wskazali tam dezinformację bezpośrednio, w szerszym spektrum wyzwań hybrydowych[33]. Deklaracja szczytu londyńskiego z 2019 r. ujmowała to zagadnienie w kontekście zagrożeń hybrydowych, które wymagają odpowiednich środków zaradczych[34]. Ze znacznie większą częstotliwością i w nowych kontekstach kwestie te pojawiły się w deklaracji szczytu w Brukseli z 2021 r., gdzie dezinformacja wspomniana została wprost jako przykład zagrożeń hybrydowych ze strony Rosji i Chin[35]. Bardziej zwięźle, choć w podobnym tonie kwestie

31 A. Ünver, A. Kurnaz, *Securitization of disinformation in NATO's lexicon: Computational text analysis*, „All Azimuth. A journal of foreign policy and peace", 21 II 2022 [preprint], s. 7: <www.dx.doi.org/10.2139/ssrn.4040148> [dostęp: 25 VII 2022].

32 *NATO's approach to countering disinformation: a focus on COVID-19*, „North Atlantic Treaty Organization" [online], 17 VII 2020 [dostęp: 22 VII 2022]: <www.nato.int/cps/en/natohq/177273.htm>.

33 Zob. *Documents talk…*, s. 562–592.

34 Tamże, s. 606–609.

35 *Brussels Summit communiqué*, „North Atlantic Treaty Organization" [online], 1 VII 2022 [dostęp: 23 VII 2022]: <www.nato.int/cps/en/natohq/news_185000.htm>.

te ujęto w deklaracji szczytu madryckiego z 2022 r.[36] 24 marca, w toku przygotowań do tego spotkania, roboczy szczyt NATO w Brukseli zdecydował o kontynuowaniu działań związanych z odpieraniem kłamstw Rosji o jej agresji na Ukrainie oraz ujawnianiem towarzyszących im wrogich operacji informacyjnych i fałszywych narracji. Postanowiono też zwiększyć wsparcie dla projektów wzmacniających społeczną odporność na dezinformację i inne zagrożenia hybrydowe[37] oraz wezwano Chiny, by zaprzestały nagłaśniać fałszywe narracje polityczne Kremla[38].

Trzy ostatnie dokumenty budowały swój przekaz, uwzględniając ustalenia obszernego raportu z 2020 r., który stanowi przegląd środowiska strategicznego NATO[39]. Dezinformacja została tam przedstawiona jako zagrożenie w czasach pokoju i wojny, skierowane przeciw demokratycznym państwom i społeczeństwom, ich siłom zbrojnym oraz wzajemnej współpracy. Rozwinięte zapisy, które mają się przełożyć na sojusznicze procesy planistyczne, zostały natomiast zawarte w *Koncepcji strategicznej NATO* z 2022 r.[40] (znalazły się tam po raz pierwszy od zakończenia zimnej wojny). Co istotniejsze, możliwe implikacje wrogich działań hybrydowych (a więc także dezinformacji) zostały wpisane w kontekst obrony kolektywnej. Krótki przegląd najważniejszych politycznych decyzji NATO odnośnie do dezinformacji zawiera poniższa tabela.

36 *Madrid Summit declaration*, „North Atlantic Treaty Organization" [online], 22 VII 2022 [dostęp: 23 VII 2022]: <www.nato.int/cps/en/natohq/official_texts_196951.htm>.

37 *Bolstering the democratic resilience of the alliance against disinformation and propaganda*, NATO Parliamentary Assembly CDS, 10 X 2021: <https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-04/013%20CDS%2021%20E%20-%20DEMOCRATIC%20RESILIENCE%20AGAINST%20DISINFORMATION%20AND%20PROPAGANDA%20-%20SANCHEZ_0.pdf> [dostęp: 23 VII 2022].

38 *Statement by NATO heads of state and government*, „North Atlantic Treaty Organization" [online], 4 VII 2022 [dostęp: 23 VII 2022]: <www.nato.int/cps/en/natohq/official_texts_193719.htm>.

39 *NATO 2030. United for a new era. Analysis and recommendations of the Reflection Group appointed by the NATO Secretary General*, [North Atlantic Treaty Organization], 25 XI 2020: <www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf> [dostęp: 1 VII 2022].

40 *NATO 2022 strategic concept*, [North Atlantic Treaty Organization], 29 VI 2022: <www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf> [dostęp: 23 VII 2022].

Tabela. Ważniejsze oświadczenia polityczne NATO ws. dezinformacji (treść i kontekst)

Dokument	Najważniejszy zapis
Deklaracja szczytu brukselskiego (2018)	We face hybrid challenges, including disinformation campaigns and malicious cyber activities
Deklaracja szczytu londyńskiego (2019)	We face cyber and hybrid threats. […] We are increasing our tools to respond to cyber attacks, and strengthening our ability to prepare for, deter, and defend against hybrid tactics that seek to undermine our security and societies
Deklaracja szczytu brukselskiego (2021)	We are increasingly confronted by cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies. […] Russia has also intensified its hybrid actions against NATO Allies and partners, including through proxies. This includes attempted interference in Allied elections and democratic processes; political and economic pressure and intimidation; widespread disinformation campaigns; malicious cyber activities; and turning a blind eye to cyber criminals operating from its territory, including those who target and disrupt critical infrastructure in NATO countries. […] We are enhancing our situational awareness and expanding the tools at our disposal to counter hybrid threats, including disinformation campaigns, by developing comprehensive preventive and response options. We will also continue to support our partners as they strengthen their resilience in the face of hybrid challenges. […] We remain concerned with China's frequent lack of transparency and use of disinformation. […] The current strategic environment and the COVID pandemic underscore the importance of NATO-EU cooperation in the face of current and evolving security challenges, in particular in addressing resilience issues, emerging and disruptive technologies, the security implications of climate change, disinformation, and the growing geostrategic competition
Deklaracja szczytu brukselskiego (2022)	We will continue to counter Russia's lies about its attack on Ukraine and expose fabricated narratives or manufactured „false flag" operations to prepare the ground for further escalation […]. We are concerned by recent public comments by PRC officials and call on China to cease amplifying the Kremlin's false narratives, in particular on the war and on NATO […]. We are ready to impose costs on those who harm us in cyberspace, and are increasing information exchange and situational awareness, enhancing civil preparedness, and strengthening our ability to respond to disinformation
Deklaracja szczytu madryckiego (2022)	We are confronted by cyber, space, and hybrid and other asymmetric threats, and by the malicious use of emerging and disruptive technologies. […] We will accelerate our adaptation in all domains, boosting our resilience to cyber and hybrid threats, and strengthening our interoperability. We will employ our political and military instruments in an integrated manner
Koncepcja strategiczna NATO (2022)	Authoritarian actors […] interfere in our democratic processes and institutions and target the security of our citizens through hybrid tactics, both directly and through proxies. They conduct malicious activities in cyberspace and space, promote disinformation campaigns, instrumentalise migration, manipulate energy supplies and employ economic coercion. […] The Russian Federation is the most significant and direct threat to Allies' security and to peace and stability in the Euro-Atlantic area. It seeks to establish spheres of influence and direct control through coercion, subversion, aggression and annexation. It uses conventional, cyber and hybrid means against us and our partners. Its coercive military posture, rhetoric and proven willingness to use force to pursue its political goals undermine the rules-based international order. […] China employs a broad range of political, economic and military tools to increase its global footprint and project power, while remaining opaque about its strategy, intentions and military build-up. The PRC's malicious hybrid and cyber operations and its confrontational rhetoric and disinformation target Allies and harm Alliance security. […] We will invest in our ability to prepare for, deter, and defend against the coercive use of political, economic, energy, information and other hybrid tactics by states and non- state actors. Hybrid operations against Allies could reach the level of armed attack and could lead the NAC to invoke Article 5 of the North Atlantic Treaty. We will continue to support our partners to counter hybrid challenges and seek to maximise synergies with other relevant actors, such as the European Union

Źródło: oprac. własne na podstawie dokumentów NATO

NATO w walce z dezinformacją – aspekty praktyczne

Praktyczne wysiłki NATO w sferze walki z dezinformacją obejmują kilka poziomów działań. W oparciu o stały mandat organizacji, wynikający z zapisów *Traktatu północnoatlantyckiego*, można tu mówić o trzech kwestiach:

– działaniach państw członkowskich na rzecz rozwoju własnych zdolności do samoobrony i pomocy sojuszniczej (art. 3),

– konsultacjach sojuszniczych (art. 4 i 9),

– kolektywnej obronie (art. 5), usankcjonowanej rozwijającym się dorobkiem decyzji politycznych władz organizacji i zapisami najnowszej edycji *Koncepcji strategicznej NATO*.

Na poziomie działalności operacyjnej sojuszu walka z dezinformacją przenika trzy główne zadania zapisane w *Koncepcji strategicznej*:

1. Kolektywną obronę i odstraszanie, której rozumienie rozszerzono w ostatnich latach do aktów agresji zwróconych nie tylko przeciw terytorium państw członkowskich, lecz także ich cyberprzestrzeni i sferze poznawczej (tj. dezinformację). Edycja strategii NATO z 2022 r. w kontekst kolektywnej obrony i odstraszania wpisuje także budowanie narodowej i sojuszniczej odporności przeciwko zagrożeniom hybrydowym. Działania sojuszu w tej dziedzinie koordynuje na potrzeby Rady Północnoatlantyckiej Komitet Odporności (Resilience Committee), pracujący na szczeblu zastępców ambasadorów[41].

2. Zarządzanie kryzysowe, gdzie przeciwdziałanie dezinformacji jest składnikiem wysiłków na rzecz zabezpieczenia przestrzeni operacyjnej wojsk i personelu cywilnego.

3. Bezpieczeństwo kooperatywne, gdzie współpraca z państwami partnerskimi i organizacjami międzynarodowymi jest elementem poprawy rozumienia otoczenia informacyjnego NATO (np. poprzez wymianę informacji) oraz synergii działań edukacyjnych i prewencyjnych, a także poprawy instrumentarium przeciwdziałania zagrożeniom hybrydowym (w tym dezinformacji).

W 2019 r. NATO przyjęło niejawny pakiet założeń i środków walki z dezinformacją, a rok później – plan mający na celu skoordynowanie przeciwdziałania szkodliwej dezinformacji dotyczącej pandemii COVID-19. W 2021 r. na potrzeby struktur sojuszniczych, państw członkowskich

41 *Resilience, and civil preparedness – Article 3*, „North Atlantic Treaty Organization" [online, dostęp: 27 VII 2022]: <www.nato.int/cps/en/natohq/topics_132722.htm?>.

i partnerskich przygotowano w Brukseli materiał szkoleniowy dotyczący zwalczania dezinformacji (*NATO toolbox for countering hostile information activities*). Zdaniem byłego szefa biura NATO w Moskwie eksponuje on dwutorowy model sojuszniczej odpowiedzi (*understand and engage*)[42]. Z jednej strony obejmuje on zrozumienie dynamiki własnego środowiska informacyjnego i służącą temu działalność analityczną – wykrywanie, analizowanie i przeciwdziałanie oraz proaktywną komunikację. W tej ostatniej kwestii kluczowe jest działanie wyprzedzające i narzucenie własnej narracji opartej na prawdzie, a także nieodpowiadanie na wrogą dezinformację własną propagandą. Z drugiej strony chodzi o działanie oparte na pozyskanej wiedzy, która pozwala właściwie kształtować własną komunikację strategiczną i działania administracyjne[43] oraz koordynować współpracę z członkami i partnerami NATO[44].

Moduł *engage* nabrał wymiaru praktycznego poprzez np. stworzenie zespołów szybkiego reagowania w sytuacjach wymagających komunikacji kryzysowej, a także rozwijanie i subsydiowanie projektów na rzecz wzmocnienia odporności społecznej na dezinformację w państwach członkowskich (także w sektorze pozarządowym). Od strony badawczej, analitycznej i edukacyjnej działania sojuszu wspierane są przez Centrum Doskonalenia ds. Komunikacji Strategicznej w Rydze, NATO Defence College w Rzymie oraz Europejskie Centrum Doskonalenia ds. Zwalczania Zagrożeń Hybrydowych z siedzibą w Helsinkach. Bezpośrednio lub pośrednio wysiłki NATO w tym obszarze wspiera również wiele ośrodków akademickich (np. Uniwersytet w Toronto, Uniwersytet Oksfordzki, Uniwersytet w Helsinkach i Massachusetts Institute of Technology) czy organizacji pozarządowych (np. Digital Forensic Lab w Atlantic Council of the United States, Alliance for Securing Democracy w German Marshall Fund, Stop Fake, Bellingcat, Friends of Ukraine i Ruch Elfów na Litwie). Najściślej

42 T. Chłoń, *NATO and countering disinformation. The need for a more proactive approach from the member states*, „Globsec" [online], 16 V 2022 [dostęp: 17 VI 2022]: <www.globsec.org/publications/15591/>.

43 Obiecującym przykładem jest wprowadzenie po rosyjskiej agresji przeciwko Ukrainie zakazu działania w krajach UE i NATO państwowych mediów rosyjskiej propagandy, jak Russia Today i Sputnik. Wcześniej przez lata podjęcie tego rodzaju kroków uniemożliwiały kwestie prawne i proceduralne.

44 *NATO's approach...*

w działaniach przeciwko dezinformacji sojusz współpracuje z Unią Europejską[45] i Organizacją Narodów Zjednoczonych.

NATO podejmuje także wysiłki na rzecz przeciwdziałania dezinformacji u źródeł problemu, korzystając w tym celu z tzw. ambasad kontaktowych w państwach spoza organizacji oraz własnych biur informacyjnych. Do końca 2021 r. zdołano utrzymać Biuro Informacji NATO w Moskwie, rozwijając tam programy i projekty skierowane do społeczeństwa obywatelskiego, mediów i środowisk naukowych. Za pomocą mediów społecznościowych rozwijano także działalność informacyjną w języku rosyjskim. Wspomniane przedsięwzięcia napotykały wiele trudności z uwagi na istniejące w Rosji administracyjne ograniczenia działalności zagranicznych podmiotów informacyjnych oraz państwową (także prawnokarną) kontrolę własnej infosfery. Na żądanie rosyjskich władz biuro NATO w Moskwie zostało zamknięte w grudniu 2021 r., co ograniczyło możliwości przedstawiania rosyjskiemu społeczeństwu rzetelnych informacji na temat sojuszu[46].

Działaniom NATO przyświeca kilka zasad tworzących swoisty kodeks postępowania w walce z dezinformacją. Opierają się one na:

– założeniu maksymalizacji wiedzy o zagrożeniach informacyjnych. Osiąga się to poprzez stały monitoring środowiska informacyjnego (pod kątem podmiotu komunikującego, treści komunikacji i oceny jej szkodliwości dla sojuszu) oraz wykrywanie zagrożeń. Pozwala to na wypracowanie odpowiedzi adekwatnych pod względem czasu, treści, wykorzystywanego przekaźnika i skali własnego przedsięwzięcia;

– zachowaniu inicjatywy i dążeniu, by docierać z własną narracją do odbiorców, a nie jedynie reagować na akty dezinformacji. Innymi słowy – aktywność informacyjna powinna się odbywać raczej na warunkach NATO niż narzucanych przez przeciwnika. Wynika to z faktu, że w dobie mediów

45 Bilans wspólnych działań: D. Zandee, S. van der Meer, A. Stoetman, *Countering hybrid threats. Steps for improving EU–NATO cooperation*, Clingendael, October 2021 (Clingendael Report): <https://www.clingendael.org/pub/2021/countering-hybrid-threats/> [dostęp: 3 VII 2022]; P. Szymański, *Towards greater resilience: NATO and the EU on hybrid threats*, Centre for Eastern Studies, Warsaw 2020 (OSW Commentary, 328).

46 Za rozmowę na temat aktywności tej struktury autor dziękuje ambasadorowi Tomaszowi Chłoniowi, szefowi Biura Informacyjnego NATO w Moskwie w latach 2017–2020.

internetowych fałsz rozprzestrzenia się szybciej i skuteczniej niż próby jego dementowania. Tym bardziej, że to ostatnie – choć niekiedy konieczne – często utrwala jedynie komunikaty dezinformatorów;

– spójności własnej narracji i wiarygodności przekazywanych informacji (opartych na sprawdzonych faktach i dowodach) oraz ich adekwatności czasowej;

– łączeniu własnych zasobów z działaniami państw członkowskich, organizacji międzynarodowych oraz sektora pozarządowego i społeczeństwa obywatelskiego.

W brukselskiej Kwaterze Głównej NATO zwalczanie wrogiej dezinformacji koordynowane jest przez dwa ośrodki:

– pion dyplomacji publicznej (PDD) w ramach Sekretariatu Międzynarodowego (IS), kierowany przez asystenta sekretarza generalnego i obejmujący odpowiedzialnością cywilne i wojskowe struktury organizacji. Jego pracownicy zajmują się pozyskiwaniem wiedzy i działalnością analityczną budującą przesłanki dla procesu decyzyjnego NATO, współpracą z partnerami zewnętrznymi (oraz innymi pionami IS), dowództwami sojuszniczymi i Międzynarodowym Sztabem Wojskowym (IMS), edukacją oraz wspieraniem państw członkowskich. Właśnie stąd wychodzą oceny polityczne i rekomendacje działań dla władz sojuszu. Można zatem stwierdzić, że działalność PDD dotyczy przede wszystkim aspektu *understand* w zakresie zwalczania dezinformacji przez sojuszników;

– aspektem *engage* zajmuje się przede wszystkim rzecznik prasowy NATO i jego biuro (pozostający formalnie w strukturze PDD). Nie tylko kształtuje i koordynuje on bieżącą działalność medialną sekretarza generalnego i organizacji, ale jest przede wszystkim punktem pierwszego kontaktu dla mediów, źródłem oświadczeń i zweryfikowanego przekazu. Zadania swoje realizuje poprzez wywiady, artykuły prasowe i komunikację w mediach społecznościowych, konferencje prasowe, oświadczenia, wykłady, przemówienia, wizyty studyjne i publikacje materiałów informacyjnych. W każdej z form komunikacyjnych dba on także o spójność przekazu NATO.

Zasadnicza odpowiedzialność za zwalczanie dezinformacji spoczywa jednak ciągle na państwach członkowskich. Pomimo że mogą one korzystać z dorobku eksperckiego i dobrych praktyk NATO, nie istnieje w tym zakresie żaden obowiązujący standard sojuszniczy. Dotyczy to zarówno organizacji, jak i form pracy narodowych ośrodków zwalczania dezinformacji.

Częste rozproszenie ich kompetencji czy wąskie obszary zainteresowań oraz skoncentrowanie się na zadaniach narodowych nie ułatwiają już nie tylko koordynacji działań z poziomu NATO, ale nawet jednolitej komunikacji. Państwa członkowskie pracują ponadto według własnych metod i nawet jeśli część z nich jest znana[47], to nie tworzą wspólnego *modus operandi*. Nie wszyscy sojusznicy mają ponadto struktury odpowiadające za walkę z dezinformacją, a niektórzy wnoszą tylko niewielki wkład do wspólnych działań. W ostatnich latach w skali całego sojuszu rośnie jednak zrozumienie dla potrzeby edukacji medialnej społeczeństw i zwiększania ich zbiorowej odporności.

Po stronie słabości natowskiego systemu zwalczania dezinformacji zapisać można także czynnik ludzki, w tym niedostatek kompetentnego personelu mającego wysokie kwalifikacje analityczne, a jednocześnie rozumiejącego politykę międzynarodową i znającego nowoczesne technologie. Ograniczenia powoduje też niedostateczne wsparcie techniczne dla działalności analitycznej i wykrywania dezinformacji. Przetworzenie olbrzymiej liczby danych w odpowiednim czasie wymaga bowiem wsparcia ekspertów zautomatyzowanym systemem analizy informacji. Od dłuższego czasu NATO pracuje nad własnymi rozwiązaniami, które pozwoliłyby na przyspieszenie wykrywania zagrożeń i poprawę procedur analitycznych wspierających procesy decyzyjne.

* * *

Sojusz Północnoatlantycki, choć doświadczony ponad siedmioma dekadami walki z dezinformacją, dopiero w ostatnich latach podjął wysiłek usystematyzowania swych działań w tym obszarze i podniesienia ich rangi politycznej. Nie przybrały one jednak dotąd charakteru strategii czy spójnego planu. NATO dostrzega wprawdzie autonomiczność i szkodliwość dezinformacji pośród innych zagrożeń hybrydowych, ale przekaz zawarty w dokumentach Rady Północnoatlantyckiej wciąż nie jest w tej mierze konsekwentny. Niewątpliwie wynika to z rozbieżności stanowisk państw członkowskich, które albo odmiennie rozkładają priorytety, albo z różną ostrością postrzegają konkretne zagrożenia (w tym dezinformację). Stąd też język komunikatów

47 Np. brytyjski RESIST czy szwedzki Countering Information Influence Activities. Szerzej zob. R. Kupiecki, F. Bryjka, T. Chłoń, *Dezinformacja…*, s. 123–138.

NATO skłonny jest raczej do generalizacji i szerokiego ujmowania zagrożeń (np. w sformułowaniach *hybrydowość* czy *360 stopni*). Łatwiej w nim o konsens polityczny i unikanie przewlekłych sporów. Krokiem w dobrą stronę są zapisy madryckiej koncepcji strategicznej z 2022 r., które dają solidne podstawy dla planowania działań cywilnych i wojskowych w tej dziedzinie, a co za tym idzie, ułatwiają systematyzację prac NATO.

W dyskusjach pojawiają się dobre propozycje zmian[48], obejmujące m.in.:

– wprowadzenie tematyki dezinformacji do planu prac ministrów oraz szefów państw i rządów NATO (co wymagałoby stosownego przygotowania debat oraz rozliczenia się NATO i państw członkowskich z podejmowanych działań),

– wzmacnianie odporności społecznej na dezinformację (np. poprzez edukację medialną, wsparcie dla organizacji pozarządowych, które walczą z dezinformacją, czy monitoring mediów i kampanii politycznych),

– poszerzenie zakresu działań prewencyjnych i ofensywnych (np. o regulacje dla mediów elektronicznych wymuszające odpowiedzialność za upubliczniane treści, sankcje dla dezinformatorów czy ujawnianie źródeł dezinformacji),

– niwelowanie różnic w praktycznym podejściu do dezinformacji w poszczególnych państwach zachodnich (np. poprzez konsultacje i dzielenie się dobrymi praktykami).

Czas pokaże, czy starczy NATO determinacji, by przystąpić do wdrażania tych postulatów. Bez wątpienia wiele doświadczeń i kompetencji mogą tu wnieść zaproszone do członkostwa Finlandia i Szwecja.

Bibliografia

Active measures. A report on the substance and process of anti-U.S. disinformation and propaganda campaigns, US State Department, August 1986: <www.insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20Substance%20and%20Process%20of%20AntiUS%20Disinformation%20August%201986.pdf> [dostęp: 1 VII 2022].

Baumann M., *Propaganda fights and disinformation campaigns: the discourse on information warfare in Russia-West relations*, „Contemporary Politics" 2020, vol. 26, No. 3, DOI: 10.1080/13569775.2020.1728612.

48 Szerzej zob. T. Chłoń, *NATO...*

Bolstering the democratic resilience of the alliance against disinformation and propaganda, NATO Parliamentary Assembly CDS, 10 X 2021: <https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-04/013%20CDS%2021%20E%20-%20DEMOCRATIC%20RESILIENCE%20AGAINST%20DISINFORMATION%20AND%20PROPAGANDA%20-%20SANCHEZ_0.pdf> [dostęp: 23 VII 2022].

Brussels Summit Communiqué, „North Atlantic Treaty Organization" [online], 1 VII 2022 [dostęp: 23 VII 2022]: <www.nato.int/cps/en/natohq/news_185000.htm>.

Bryjka F., *Wojny zastępcze*, Polski Instytut Spraw Międzynarodowych, Warszawa 2021.

Chłoń T., *NATO and countering disinformation. The need for a more proactive approach from the member states*, „Globsec" [online], 16 V 2022 [dostęp: 17 VI 2022]: <www.globsec.org/publications/15591/>.

Disinformation, narratives and memory politics in Russia and Belarus, ed. A. Legucka, R. Kupiecki, Routledge, London 2022.

Documents talk. NATO–Russia relations after the Cold War, ed. R. Kupiecki, M. Menkiszak, Polish Institute of International Affairs, Warsaw 2020.

Foreign Service Dispatch 116 of September 8, 1952, US Embassy Moscow, The Soviet Union and the Atlantic Pact, [w:] G. F. Kennan, *Memoirs 1950–1963*, Little Brown, Boston 1971.

Galeotti M., *Controlling chaos. How Russia manages its political war in Europe*, European Council of Foreign Relations, 1 IX 2017: <www.ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/> [dostęp: 23 VI 2022].

Galeotti M., *The „Gerasimov Doctrine" and Russian non-linear war*, „In Moscow's Shadows" [online], 7 X 2015 [dostęp: 14 VI 2022]: <www.inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>.

Galeotti M., *The mythical „Gerasimov Doctrine" and the language of threat*, „Critical Studies on Security" 2019, vol. 7, No. 2, DOI: 10.1080/21624887.2018.1441623.

Galeotti M., *Russian political war. Moving beyond the hybrid*, Routlegde, London–New York 2019.

Gerrits A. W. M., *Disinformation in international relations. How important is it?*, „Security and Human Rights" 2018, vol. 29, DOI: 10.1163/18750230-02901007.

Giles K., *Handbook of Russian information warfare*, NATO Defence College, Rome 2016 (Fellowship Monograph, 9): <www.researchgate.net/publication/313423985_Handbook_of_Russian_Information_Warfare> [dostęp: 11 IV 2022].

Giles K., Seaboyer A., *The Russian information warfare construct*, Royal Military College, Kingston, March 2019: <https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf> [dostęp: 22 VII 2022].

Kennan G. F., *Memoirs 1950–1963*, Little Brown, Boston 1971.

Kucharski L., *Russian multi-domain strategy against NATO. Information, confrontation and US forward-deployed nuclear weapons in Europe*, U.S. Department of Energy, Office of Scientific and Technical Information, 2018, DOI: 10.2172/1635758: <www.osti.gov/servlets/purl/1635758> [dostęp: 4 VII 2022].

Kupiecki R., *„Mit założycielski" polityki zagranicznej Rosji*, „Sprawy Międzynarodowe" 2019, t. 72, nr 4, DOI: 10.35757/SM.2019.72.4.03.

Kupiecki R., *Siła i solidarność. Strategia NATO 1949–1989*, Polski Instytut Spraw Międzynarodowych, Warszawa 2012.

Kupiecki R., Bryjka F., Chłoń T., *Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przeciwdziałanie*, Wydawnictwo Naukowe „Scholar", Warszawa 2022.

Kux D., *Soviet active measures and disinformation. Overview and assessment*, „Parameters" 1985, No. 4.

Lanoszka A., *Disinformation in international politics*, „European Journal of International Security" 2019, vol. 4, issue 2, DOI: 10.1017/eis.209.6.

Madrid Summit declaration, „North Atlantic Treaty Organization" [online], 22 VII 2022 [dostęp: 23 VII 2022]: <www.nato.int/cps/en/natohq/official_texts_196951.htm>.

Modus trollerandi, p. 1–7, „EU vs Disinfo" [online, dostęp: 20 VII 2022]: <https://euvsdisinfo.eu/?s=modus+trollerandi>.

Najzer B., *The hybrid age. International security in the era of hybrid warfare*, Bloomsbury Publishing, London 2020.

NATO 2022 strategic concept, [North Atlantic Treaty Organization], 29 VI 2022: <www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf> [dostęp: 23 VII 2022].

NATO 2030. United for a new era. Analysis and recommendations of the Reflection Group appointed by the NATO Secretary General, [North Atlantic Treaty Organization], 25 XI 2020: <www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf> [dostęp: 1 VII 2022].

NATO strategy documents 1949–1969, ed. G. D. Pedlow, Historical Office SHAPE, NATO International Staff Central Archives, Brussels 1997.

NATO's approach to countering disinformation: a focus on COVID-19, „North Atlantic Treaty Organization" [online], 17 VII 2020 [dostęp: 22 VII 2022]: <www.nato.int/cps/en/natohq/177273.htm>.

NATO's response to hybrid threats, „North Atlantic Treaty Organization" [online], 21 VI 2022 [dostęp: 25 VII 2022]: <www.nato.int/cps/en/natohq/topics_156338.htm>.

Nimmo B., *Anatomy of an info-war. How Russia's propaganda machine works and how to counter it*, „Stop Fake" [online], 19 V 2015 [dostęp: 22 VII 2022]: <www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it>.

Pacepa I. M., Rychlak J. R., *Dezinformacja: były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu*, przeł. M. Machnik, Editio, Gliwice 2015.

Paul Ch., Matthews M., *The Russian „firehose of falsehood" propaganda model. Why it might work and options to counter it*, RAND Corporation, 2016, DOI: 10.7249/PE198: <www.rand.org/pubs/perspectives/PE198.html> [dostęp: 23 VII 2022].

Radin A., Demus A., Marcinek K., *Understanding Russian subversion. Patterns, threat and responses*, RAND Corporation, 2020, DOI: 10.7249/PE331: <www.rand.org/pubs/perspectives/PE331.html> [dostęp: 19 VII 2022].

Resilience, and civil preparedness – Article 3, „North Atlantic Treaty Organization" [online, dostęp: 27 VII 2022]: <www.nato.int/cps/en/natohq/topics_132722.htm?>.

Rid T., *Wojna informacyjna*, przeł. M. Tyl, Bellona, Warszawa 2020.

Sorrels C. A., *Soviet propaganda campaign against NATO*, US Arms Control and Disarmament Agency, Washington DC, October 1983: <www.insidethecoldwar.org/sites/default/files/documents/Soviet%20Propaganda%20Campaign%20Against%20NATO_0.pdf> [dostęp: 21 VII 2022].

Statement by NATO heads of state and government, „North Atlantic Treaty Organization" [online], 4 VII 2022 [dostęp: 23 VII 2022]: <www.nato.int/cps/en/natohq/official_texts_193719.htm>.

Szymański P., *Towards greater resilience: NATO and the EU on hybrid threats*, Centre for Eastern Studies, Warsaw 2020 (OSW Commentary, 328).

Treverton G., Thvedt A., Chen A. R., Lee K., McCue M., *Addressing hybrid threats*, Swedish Defense University, Stockholm 2018.

Ünver A., Kurnaz A., *Securitization of disinformation in NATO's lexicon. Computational text analysis*, „All Azimuth. A journal of foreign policy and peace", 21 II 2022 [preprint]: <www.dx.doi.org/10.2139/ssrn.4040148> [dostęp: 25 VII 2022].

Volkoff V., *Dezinformacja. Oręż wojny*, przeł. A. Arciuch, Delikon, Warszawa 1991.

Volkoff V., *Petite histoire de la désinformation. Du cheval de troie à internet, le rocher*, Éditions du Rocher, Paris 1999.

What is disinformation?, „Prevency" [online, dostęp: 11 VII 2022]: <www.prevency.com/en/what-is-disinformation>.

Wilson A., *Four types of Russian propaganda*, „Aspen Review" [online], 15 III 2017 [dostęp: 20 VII 2022]: <www.aspen.review/article/2017/four-types-of-russian-propaganda/>.

Wojnowski M., *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12.

Zandee D., Meer S. van der, Stoetman A., *Countering hybrid threats. Steps for improving EU–NATO cooperation*, Clingendael, October 2021 (Clingendael Report): <https://www.clingendael.org/pub/2021/countering-hybrid-threats/> [dostęp: 3 VII 2022].