Komentarze OSW

OŚRODEK STUDIÓW WSCHODNICH **NUMER 328** 24.04.2020 **www.osw.waw.pl**

NATO i Unia Europejska wobec zagrożeń hybrydowych

Piotr Szymański

W ostatnich latach wzrosło znaczenie NATO i Unii Europejskiej w zwalczaniu zagrożeń hybrydowych ze strony państw i aktorów niepaństwowych. Kategoria ta obejmuje szerokie spektrum operacji militarnych i niemilitarnych – od wykorzystania sił specjalnych i grup dywersyjnych po dezinformację i ataki cybernetyczne. NATO i UE zaangażowane są w koordynację współpracy międzynarodowej w zwalczaniu zagrożeń hybrydowych, a także ochronę własnych struktur przed nimi. Obie organizacje wspierają w ten sposób działania na poziomie narodowym, gdyż to poszczególne kraje ponoszą główny ciężar odpowiedzialności za reagowanie na tego typu wyzwania. Skuteczność NATO i UE ograniczają jednak niedostateczne środki finansowe na przeciwdziałanie zagrożeniom hybrydowym. Negatywnie wpływa na nią także brak woli państw członkowskich do zwiększenia wymiany informacji wrażliwych, dotyczących np. ochrony infrastruktury krytycznej czy cyberbezpieczeństwa. Przykład nasilenia wymierzonych w Zachód kampanii dezinformacyjnych w związku z pandemią COVID-19 dowodzi, że NATO i UE powinny poświęcać problematyce zagrożeń hybrydowych jeszcze większą uwagę.

Rola NATO i UE w zwalczaniu zagrożeń hybrydowych

NATO i UE postrzegają zagrożenia hybrydowe w podobny sposób. Według NATO są to „działania militarne i niemilitarne oraz jawne i niejawne środki, obejmujące dezinformację, ataki cybernetyczne, presję ekonomiczną, użycie nieregularnych grup zbrojnych i wojsk regularnych". Mają na celu „rozmywanie granicy między wojną i pokojem oraz dezorientowanie społeczeństw"[1]. Unijna definicja jest bardziej rozbudowana – zagrożenia hybrydowe to „połączenie działań konwencjonalnych 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" („trudne do wykrycia i przypisania", „dezorientujące i hamujące procesy decyzyjne") wymierzone w „krytyczne słabe punkty". Zagrożenia hybrydowe „rozciągają się od ataków cybernetycznych na krytyczne systemy informacyjne, przez zakłócanie usług krytycznych (np. dostaw energii czy finansowych), do podważania zaufania społecznego do instytucji rządowych i pogłębiania podziałów społecznych"[2].

[1] *NATO's response to hybrid threats*, NATO, 8.08.2019, www.nato.int.

[2] *A Europe that Protects: Countering Hybrid Threats*, EEAS, 13.06.2018, www.eeas.europa.eu.

OSW

Ośrodek Studiów Wschodnich im. Marka Karpia
ul. Koszykowa 6a, 00-564 Warszawa
tel.: (+48) 22 525 80 00, info@osw.waw.pl
www.osw.waw.pl

REDAKCJA MERYTORYCZNA: Mateusz Gniazdowski
REDAKCJA: Tomasz Strzelczyk, Szymon Sztyk
SKŁAD: Wojciech Mańkowski

Zagrożenia hybrydowe to zatem pojemny termin, obejmujący szeroki wachlarz działań destabilizujących różnego typu. Nieostra definicja z jednej strony podnosi ryzyko „rozmywania" dyskusji, z drugiej zaś sprzyja debacie, gdyż poszczególne państwa mogą włączać do niej kwestie o priorytetowym znaczeniu z ich perspektywy. Przykładami zagrożeń hybrydowych będą więc zarówno operacje kinetyczne, np. użycie nieoznakowanych żołnierzy do opanowania jakiegoś terytorium, działania wymierzone w infrastrukturę krytyczną (m.in. cyberataki czy paraliżowanie łączności GPS), organizacja zamachu stanu czy zabójstwa realizowane na zlecenie obcych służb specjalnych, jak i niekinetyczne, np. szeroki zakres czynności dezinformacyjnych i propagandowych, sponsorowanie radykalnych ruchów politycznych, stosowanie presji ekonomicznej czy też niejawne działania mające sprzyjać narastaniu kryzysu politycznego w innych państwach (np. korumpowanie polityków).

Pierwszoplanową rolę w zwalczaniu zagrożeń hybrydowych odgrywają państwa członkowskie NATO i UE. To 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. Są też najbliżej potencjalnych zagrożeń, co – w połączeniu z krótszym niż w przypadku organizacji międzynarodowych procesem decyzyjnym – sprawia, że mogą reagować szybciej na wrogie działania hybrydowe. Ponadto zapewnienie bezpieczeństwa wewnętrznego stanowi żywotny interes każdego państwa. Oznacza to, że poszczególne rządy są bardziej niż struktury ponadnarodowe zainteresowane budowaniem odporności na zagrożenia hybrydowe.

NATO i UE zaangażowały się w zwalczanie tego typu zagrożeń ze względu na rosnące obawy przed terroryzmem związane z powstaniem Państwa Islamskiego, nasilającą się wojnę informacyjną i ingerencje w procesy wyborcze (głównie ze strony Rosji) oraz coraz dotkliwsze ataki cybernetyczne. W obszarze zagrożeń hybrydowych obie organizacje stawiają sobie zadania ochrony własnych struktur, procesów decyzyjnych i infrastruktury, a względem państw członkowskich chcą odgrywać rolę pomocniczą (subsydiarną), angażując się tam, gdzie działania na poziomie narodowym są niewystarczające. Dotyczy to m.in. budowania wspólnej świadomości sytuacyjnej. NATO i UE dążą do wzmacniania współpracy międzynarodowej w zwalczaniu zagrożeń hybrydowych (w tym także współpracy między NATO i UE), utrudnionej przez różne postrzeganie i ocenę zagrożeń przez państwa członkowskie.

> **NATO i UE stawiają na ochronę własnych struktur, procesów decyzyjnych i infrastruktury, a względem państw członkowskich chcą odgrywać rolę pomocniczą.**

Skutkuje to ich zaangażowaniem w wymianę doświadczeń i poszerzanie wiedzy na ten temat oraz w organizację ćwiczeń uwzględniających różne scenariusze konfliktu hybrydowego. Ponadto rolą obu organizacji jest wyznaczanie wspólnych standardów i minimalnych wymogów w zakresie zwalczania takich zagrożeń. Ma to na celu wyeliminowanie słabych ogniw na poziomie narodowym, rzutujących na szeroko rozumiane bezpieczeństwo europejskie i transatlantyckie (np. w obszarze cyberbezpieczeństwa, sektora finansowego, wykorzystywanego do prania pieniędzy, czy ochrony kluczowej infrastruktury energetycznej).

Od rosyjskiej agresji na Ukrainę w 2014 r. wysiłki NATO koncentrują się głównie na odbudowie zdolności do prowadzenia dużej operacji obrony zbiorowej w ramach art. 5 traktatu waszyngtońskiego. Jednak konsekwentnie realizowane przez Rosję działania pozamilitarne (m.in. ingerencja w wybory w USA w 2016 r., atak z użyciem broni chemicznej w Wielkiej Brytanii, próby zablokowania członkostwa Czarnogóry w NATO) sprawiły, że wzmocnienie odporności na niemilitarne zagrożenia stało się istotnym uzupełnieniem wojskowej adaptacji Sojuszu do nowych wyzwań. Ważnym sygnałem była deklaracja szczytu NATO w Warszawie w 2016 r., w której zapisano, że „NATO jest gotowe udzielić wsparcia państwu członkowskiemu na każdym etapie kampanii hybrydowej, Sojusz i sojuszni-

cy będą przygotowani do zwalczania wojennych działań hybrydowych w ramach obrony zbiorowej, a Rada Północnoatlantycka może uruchomić art. 5 traktatu waszyngtońskiego" (punkt 72)[3]. Aby zwiększyć zdolność do reagowania na zagrożenia hybrydowe w wymiarze militarnym (np. przez wykorzystanie grup dywersyjnych i żołnierzy bez insygniów), Sojusz postawił na poprawę zdolności wywiadowczych i szybkości działań wzmocnionych Sił Odpowiedzi NATO (VJTF). Względem zagrożeń niemilitarnych natomiast koncentruje się on przede wszystkim na cyberbezpieczeństwie.

> **Kraje członkowskie są ostrożne w kwestii udostępniania danych wywiadowczych w NATO z powodu niedostatecznego poziomu zaufania oraz obaw o bezpieczeństwo danych.**

UE jest coraz bardziej zaniepokojona zagrożeniami hybrydowymi. Od 2014 r. przyjęła ponad 20 różnego typu dokumentów odnoszących się do tego zagadnienia. Dotyczyły one m.in.: zwalczania broni masowego rażenia, bezpieczeństwa dostaw energii, bezpieczeństwa morskiego, ochrony danych, ochrony unijnych granic, przestrzeni kosmicznej czy zagranicznych inwestycji bezpośrednich[4]. Dodatkowo UE ma własny program ochrony infrastruktury krytycznej oparty na Dyrektywie ws. rozpoznania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (2008). Jednak w ostatnich latach największe znaczenie w budowaniu unijnej odporności na zagrożenia hybrydowe zyskały wzmacnianie świadomości sytuacyjnej i cyberbezpieczeństwa oraz walka z dezinformacją. W 2019 r. Rada UE uznała, że „kraje członkowskie mają możliwość aktywowania unijnej klauzuli solidarności (art. 222 Traktatu o funkcjonowaniu UE) w odpowiedzi na poważny kryzys wynikający z aktywności hybrydowej"[5].

Priorytety NATO: świadomość sytuacyjna, cyberobrona i ćwiczenia

(1) Natowskie wsparcie dla państw członkowskich w zakresie reagowania na działania hybrydowe obejmuje monitorowanie i analizę zagrożeń, wymianę informacji wywiadowczych i doświadczeń krajowych oraz zapewnianie wspólnej świadomości sytuacyjnej. Ważnymi wydarzeniami były stworzenie w 2017 r. wydziału ds. analiz zagadnień hybrydowych (w tym cybernetycznych) w nowym Połączonym Pionie Wywiadu i Bezpieczeństwa (Joint Intelligence and Security Division, JISD) w Kwaterze Głównej NATO, który powstał w ramach reformy natowskiego wywiadu, oraz wzmocnienie cywilno-wojskowej współpracy wywiadowczej. Zadaniem wydziału jest całościowa analiza zagrożeń dla obszaru transatlantyckiego, uwzględniająca różne aspekty militarnych i niemilitarnych działań hybrydowych. Jego powstanie stanowi jednak dopiero wstęp do poprawy wspólnej świadomości sytuacyjnej w zakresie tego typu zagrożeń. NATO nie dysponuje własną służbą wywiadowczą, polega jedynie na danych uzyskanych przez poszczególne agencje narodowe. Kraje członkowskie są zaś ostrożne w kwestii udostępniania informacji wywiadowczych na forum Sojuszu. Wynika to m.in. z niedostatecznego poziomu zaufania oraz obaw o bezpieczeństwo danych[6]. W praktyce bardziej zaawansowana wymiana informacji wywiadowczej odbywa się w ramach współpracy dwustronnej lub w mniejszych grupach państw.

(2) Od 2018 r. NATO dysponuje też zespołami wspomagającymi ds. zwalczania zagrożeń hybrydowych (Counter Hybrid Support Teams, CHST). Wchodzący w ich skład eksperci mają udzielać doraźnej pomocy i doradzać władzom państwa, w którym ma miejsce kryzys hybrydowy. W listopadzie 2019 r. mechanizm ten został uruchomiony po raz pierwszy przez Czarnogórę – chce ona skorzystać z natowskich doświadczeń w zwalczaniu zagrożeń hybrydowych ze strony Rosji

[3] *Warsaw Summit Communiqué*, NATO, 9.07.2016, www.nato.int.

[4] D. Fiott, R. Parkes, *Protecting Europe: the EU's response to hybrid threats*, European Union Institute for Security Studies, 2019.

[5] *Complementary efforts to enhance resilience and counter hybrid threats – Council Conclusions*, The Council of the European Union, 10.12.2019, data.consilium.europa.eu.

[6] J. Ballast, *Trust (in) NATO – The future of intelligence sharing within the Alliance*, NATO Defense College, Research Paper, No. 140, September 2017, www.ndc.nato.int.

do zabezpieczenia wyborów parlamentarnych w 2020 r. (w Czarnogórze doszło w 2016 r. do zorganizowanej przez Rosję próby zamachu stanu). Misja zespołu, wspieranego też przez ekspertów z USA, koncentrowała się na zmianach w ustawodawstwie i cyberbezpieczeństwie[7]. W otwartych źródłach nie ma informacji na temat innych przykładów zaangażowania CHST. Być może kraje członkowskie nie doświadczyły dotychczas działań hybrydowych, których skala wymagałyby zwrócenia się o pomoc do natowskich ekspertów. Innym wytłumaczeniem może być niechęć państw członkowskich do ujawniania słabych punktów swoich systemów bezpieczeństwa lub wątpliwości co do możliwości uzyskania szybkiej i skutecznej pomocy w sytuacji kryzysowej.

(3) NATO traktuje zagrożenia cybernetyczne jako coraz ważniejsze zagadnienie, o czym świadczy uznanie cyberprzestrzeni za jedną z domen operacyjnych (analogicznie do lądowej, morskiej czy powietrznej) na szczycie w Warszawie w 2016 r., a także stwierdzenie z deklaracji ze szczytu w Newport w 2014 r. o tym, że atak cybernetyczny może skutkować uruchomieniem art. 5[8]. NATO w cyberprzestrzeni odgrywa potrójną rolę – motywuje państwa członkowskie do większych inwestycji w cyberbezpieczeństwo, jest platformą wymiany informacji i szkoleniową oraz zabezpiecza własne sieci i wspiera bezpieczeństwo sieci krajowych.

W 2016 r. sojusznicy przyjęli zobowiązanie ws. obrony cybernetycznej (Cyber Defence Pledge), według którego państwa członkowskie mają wzmacniać zdolności niezbędne do obrony swojej infrastruktury i sieci teleinformatycznej oraz zapewnić odpowiedni poziom nakładów finansowych na cyberobronę (nie został on jednak precyzyjnie określony jako procent budżetu obrony)[9]. W ostatnich latach wśród europejskich sojuszników największe inwestycje w cyberbezpieczeństwo realizują Wielka Brytania (1,9 mld funtów w latach 2016–2021) i Francja (1,6 mld euro w latach 2019–2025). Państwa członkowskie rozwijają też na poziomie narodowym zdolności do działań ofensywnych w cyberprzestrzeni. Gotowość ich udostępnienia na potrzeby NATO zadeklarowało dotychczas dziewięć krajów[10]. W zakresie ćwiczeń i ekspertyzy NATO polega na utworzonym w 2008 r. Centrum Doskonalenia Obrony przed Cyberatakami w Tallinnie (NATO CCD COE). Jest ono organizatorem głównych corocznych natowskich ćwiczeń obrony cybernetycznej Locked Shields.

> **NATO traktuje zagrożenia cybernetyczne jako coraz ważniejsze zagadnienie, o czym świadczy uznanie cyberprzestrzeni za jedną z domen operacyjnych.**

Z kolei za ochronę sieci Sojuszu odpowiada Zespół Reagowania na Incydenty Komputerowe (NCIRC), liczący ok. 200 ekspertów. NCIRC ma też zdolność wsparcia ochrony sieci krajów członkowskich poprzez wydzielenie zespołów szybkiego reagowania cybernetycznego, które mogą udzielić pomocy państwu będącemu obiektem ataku cybernetycznego w ciągu 24 godzin.

W 2018 r. NATO utworzyło Centrum Operacji w Cyberprzestrzeni. Ma ono odpowiadać za budowanie wspólnej świadomości sytuacyjnej Sojuszu dotyczącej zagrożeń cybernetycznych, koordynację aktywności państw członkowskich w cyberprzestrzeni, a także zabezpieczenie natowskich operacji i misji. Pełną zdolność operacyjną osiągnie ono jednak dopiero w 2023 r., co może być związane z trudnościami w rekrutacji specjalistów (konkurencja z sektorem prywatnym). Czynnikiem wyhamowującym współpracę jest też nastawienie

[7] S. Lekic, *First NATO counter-hybrid warfare team to deploy to Montenegro*, Stars and Stripes, 8.11.2019, www.stripes.com.

[8] *Warsaw Summit Communiqué*, *op. cit.* „Cyberataki mogą osiągnąć poziom grożący dobrobytowi, bezpieczeństwu i stabilności na poziomie narodowym i obszaru euroatlantyckiego. Ich wpływ na nowoczesne społeczeństwa może być tak szkodliwy, jak w przypadku ataku konwencjonalnego. W związku z tym potwierdzamy, że cyberobrona jest częścią kluczowego zadania NATO – obrony zbiorowej. Decyzja odnośnie do tego, kiedy cyberatak doprowadzi do uruchomienia art. 5, będzie podejmowana przez Radę Północnoatlantycką indywidualnie dla każdego przypadku". *Wales Summit Declaration*, NATO, 5.09.2014, www.nato.int.

[9] *Cyber Defence Pledge*, NATO, 8.07.2016, www.nato.int.

[10] USA, Wielka Brytania, Holandia, Estonia, Norwegia, Niemcy, Francja, Dania i Litwa. S. Vavra, *NATO cyber-operations center will be leaning on its members for offensive hacks*, Cyberscoop, 30.09.2019, www.cyberscoop.com.

samych krajów członkowskich – te z nich, które zainwestowały najwięcej w cyberbezpieczeństwo, nie są skłonne dzielić się technologiami z tymi, które na nim oszczędzały[11]. Ponadto eksperci wskazują na brak planów rozwoju natowskich zdolności ofensywnych w cyberprzestrzeni (odpowiadają za nie poszczególne kraje, które kierują się różnymi strategiami), a także brak faktycznego dowództwa cybernetycznego, wypracowującego wspólną doktrynę oraz planującego i integrującego zdolności[12]. Istnieje też obawa o to, że ze względu na skalę problemu NATO zawsze będzie pozostawać w tyle za podmiotami prowadzącymi wrogą działalność w cyberprzestrzeni. Stąd coraz większą rolę odgrywa współpraca z sektorem prywatnym w ramach mechanizmów takich jak natowska platforma Malware Information Sharing Platform (udostępniająca firmom informacje na temat złośliwego oprogramowania) czy program współpracy Agencji Komunikacji i Informacji NATO (NCIA) z podmiotami z branży cyberbezpieczeństwa.

> **W NATO brakuje myślenia o działaniach ofensywnych w cyberprzestrzeni oraz faktycznego dowództwa cybernetycznego, wypracowującego wspólną doktrynę i planującego rozwój zdolności.**

(4) Istotnym elementem natowskiej strategii przeciwdziałania zagrożeniom hybrydowym są ćwiczenia. Sojusz stosuje tu dwutorowe podejście. Z jednej strony od 2016 r. uwzględnia scenariusze hybrydowe w corocznych sztabowych ćwiczeniach zarządzania kryzysowego CMX, które testują funkcjonowanie polityczno-wojskowych procesów konsultacyjnych i decyzyjnych w NATO. Z drugiej strony sprawdza zdolność reagowania na zagrożenia hybrydowe podczas ćwiczeń poligonowych (m.in. w trakcie ćwiczeń sił odpowiedzi NATO Trident Juncture i natowskiej „szpicy" Brilliant/Noble Jump). Realizowane zadania obejmują m.in. ochronę infrastruktury krytycznej czy działania antydywersyjne (np. zwalczanie uzbrojonych grup sabotażowo-dywersyjnych w terenie zurbanizowanym).

Priorytety UE: świadomość sytuacyjna, cyberbezpieczeństwo, dezinformacja

(1) UE dąży do zwiększenia możliwości wymiany i analizy informacji na temat zagrożeń hybrydowych na potrzeby instytucji unijnych i państw członkowskich. W 2016 r. utworzono Komórkę UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych, działającą w strukturze Centrum Analiz Wywiadowczych UE. Zajmuje się ona analizą informacji i gromadzeniem danych o zagrożeniach hybrydowych na terytorium UE i w jej sąsiedztwie. Lepszemu ich zrozumieniu i wypracowaniu dobrych praktyk w ich zwalczaniu służy powstałe w 2017 r. Europejskie Centrum ds. Zwalczania Zagrożeń Hybrydowych. Ta zlokalizowana w Helsinkach instytucja – otwarta dla państw UE i NATO – pełni *de facto* rolę platformy analitycznej prowadzącej międzynarodową działalność badawczo-szkoleniową. Można zakładać, że wymiana informacji wywiadowczych w ramach UE staje w obliczu podobnych trudności jak w przypadku NATO.

(2) Zaangażowanie na rzecz bezpiecznej cyberprzestrzeni odgrywa coraz większą rolę w unijnych zmaganiach z zagrożeniami hybrydowymi. Od odporności krajowych systemów teleinformatycznych zależy nie tylko ochrona infrastruktury krytycznej w państwach UE, lecz także funkcjonowanie jednolitego rynku. Pokazały to dwa duże ataki cybernetyczne z 2017 r. – WannaCry i NotPetya[13]. Pierwszy z nich zakłócił działalność m.in. brytyjskiej służby zdrowia, niemieckich kolei (DB), francuskiego koncernu Renault i hiszpańskiego operatora Telefónica. Celem drugiego była przede wszystkim Ukraina, ale poważne straty finansowe (szacowane nawet na 300 mln dolarów) poniósł też duński A.P. Møller-Mærsk.

[11] M. Veenendaal, K. Kaska, P. Brangetto, *Is NATO Ready to Cross the Rubiconon Cyber Defence?*, CCDCOE, Tallinn 2016, ccdcoe.org.

[12] S. Arts, *Offense as the New Defense: New Life for NATO's Cyber Policy*, GMF, 13.12.2018, www.gmfus.org.

[13] D. Fiott, R. Parkes, *op. cit.*

Przełomem w podejściu UE do cyberbezpieczeństwa było przyjęcie w 2016 r. pierwszego wspólnotowego aktu prawnego w tym obszarze – Dyrektywy ws. bezpieczeństwa sieci i systemów informatycznych. W rezultacie Unia zaczęła odgrywać rolę regulatora – Bruksela zobligowała kraje członkowskie do zagwarantowania minimalnych wspólnych standardów cyberbezpieczeństwa. Dyrektywa zobowiązywała je do przyjęcia narodowych strategii bezpieczeństwa cybernetycznego, utworzenia zespołów reagowania na incydenty komputerowe (CERT) oraz europejskiej sieci CERT (wymiana informacji i koordynowanie odpowiedzi na incydenty). Ponadto Unia nałożyła na operatorów kluczowych usług (z sektorów energetyki, transportu, bankowości i finansów, służby zdrowia, zaopatrzenia w wodę, infrastruktury cyfrowej) i dostawców usług cyfrowych (internetowych platform handlowych, wyszukiwarek, chmur) obowiązek raportowania cyberincydentów[14].

Aktywność regulacyjną UE uzupełniają działania obliczone na „odstraszanie" w cyberprzestrzeni i wzmocnienie wojskowych zdolności w zakresie cyberobrony. W 2019 r. Bruksela wprowadziła możliwość nakładania sankcji (m.in. zakazu wjazdu na teren UE i zamrożenia aktywów) na osoby fizyczne i prawne spoza obszaru wspólnoty, które dopuściły się cyberataków[15]. Sankcje mogą stać się ważnym narzędziem w walce z agresywnymi działaniami w cyberprzestrzeni, za którymi stoją sponsorowane przez państwa grupy hakerskie. Natomiast od 2017 r., dzięki mechanizmowi stałej współpracy strukturalnej (PESCO) w ramach WPBiO, cyberobronie poświęconych jest kilka projektów, które dotyczą wzmocnienia zdolności do reagowania na cyberincydenty, koordynacji działań w cyberprzestrzeni, wymiany informacji o cyberzagrożeniach i powstania cyberakademii.

W obszarze cyberbezpieczeństwa Unia, poza ochroną własnych sieci (CERT-EU), wspiera też działalność badawczą i współpracę publiczno-prywatną. Zadania te realizują Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA), zajmująca się doradztwem i badaniami, oraz utworzona w 2016 r. Europejska Organizacja ds. Cyberbezpieczeństwa (ECSO), dbająca o rozwój współpracy sektora prywatnego, Komisji Europejskiej i krajów członkowskich.

> **Dezinformacja znalazła się w polu uwagi UE ze względu na manipulowanie procesami wyborczymi przez zewnętrznych aktorów oraz działalność organizacji terrorystycznych.**

Mimo wspomnianych działań dotychczasowa współpraca państw UE w obszarze cyberbezpieczeństwa rozwija się poniżej poziomu ambicji KE. Wynika to z traktowania przez nie danych na temat cyberataków jako informacji wrażliwych. Ponadto, w porównaniu do przedsięwzięć na szczeblu krajowym, zaangażowanie Unii w cyberprzestrzeni pozbawione jest odpowiedniego zaplecza finansowego – jak w przypadku agencji ENISA, od lat zabiegającej o zwiększenie budżetu i liczby pracowników. Współpracy nie ułatwiają też krajowe różnice w podejściu do cyberbezpieczeństwa, np. w zakresie współpracy z chińskimi podmiotami przy budowie sieci 5G.

(3) Dezinformacja definiowana jest przez UE jako „weryfikowalnie fałszywa lub myląca informacja tworzona, przedstawiana i rozprzestrzeniana dla korzyści ekonomicznej bądź intencjonalnego zwodzenia opinii publicznej"[16]. 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 oraz współpraca z platformami internetowymi[17].

[14] M. Grzybowski, *9 faktów o Dyrektywie NIS, które powinieneś znać*, Fundacja Bezpieczna Cyberprzestrzeń, 15.11.2016, www.cybsecurity.org. Dyrektywę uzupełnił Akt o cyberbezpieczeństwie (2019), wprowadzający jednolite unijne standardy bezpieczeństwa produktów i usług teleinformatycznych.

[15] *Cyber-attacks: Council is now able to impose sanctions*, The Council of the European Union, 17.05.2019, www.consilium.europa.eu.

[16] *Tackling online disinformation*, European Commission, www.ec.europa.eu.

[17] Unia przyjęła szereg aktów miękkiego prawa wspólnotowego w zakresie walki z dezinformacją.

W ostatnich latach UE opracowała swój „system" wykrywania dezinformacji. Jako pierwsza w 2015 r. utworzona została w Europejskiej Służbie Działań Zewnętrznych (ESDZ) grupa zadaniowa East Stratcom, analizująca i naświetlająca przykłady prokremlowskiej dezinformacji. Oprócz niej Unia dysponuje jeszcze dwoma grupami zadaniowymi, ukierunkowanymi na południowe sąsiedztwo i Bałkany Zachodnie. Przy okazji wyborów do Parlamentu Europejskiego w 2019 r. utworzono też unijną sieć podmiotów weryfikujących fakty (*fact-checking*), a także mechanizm wczesnego ostrzegania przed dezinformacją – Rapid Alert System. Jego zadaniem jest blokowanie działań dezinformacyjnych o dużej skali, jednak nie został on jeszcze uruchomiony przez żadne państwo[18]. Choć walka z dezinformacją stała się sztandarowym hasłem UE, wypracowany dotychczas system ma poważne luki – nie obejmuje przeciwdziałania szerzeniu dezinformacji przez podmioty wewnątrzunijne, co ogranicza skuteczność wprowadzanych rozwiązań. Ponadto nowo powstałe instytucje nie mają zapewnionego dostatecznego finansowania i kadr. Stąd na przykład powracające apele ze strony ekspertów i europosłów w sprawie konieczności wzmocnienia East Stratcom, liczącego tylko kilkanaście osób (ostatnio w związku z działaniami dezinformacyjnymi wokół pandemii COVID-19)[19].

Problemem jest też defensywne podejście do dezinformacji, oparte przede wszystkim na monitoringu i dementowaniu. W unijnej strategii brakuje kreowania własnej narracji osłabiającej wiarygodność podmiotów odpowiedzialnych za jej szerzenie – np. w formie publicznych wystąpień europosłów czy systematycznych kampanii medialnych o dużym zasięgu.

O sukcesie bądź niepowodzeniu unijnej walki z dezinformacją przesądzi jednak współpraca publiczno-prywatna z największymi platformami internetowymi, dobrowolnymi sygnatariuszami wspólnotowego Kodeksu postępowania w zakresie dezinformacji (2019). Są nimi: Google, Facebook, Twitter i Mozilla. Ambicją UE, zaniepokojonej skalą wykorzystania podmiotów tego typu do prowadzenia działań dezinformacyjnych, jest egzekwowanie transparentności (reklamy politycznej, polityki reklamowej, działania algorytmów dobierających wiadomości) oraz wprowadzenie rozwiązań służących oznaczaniu botów i usuwaniu fałszywych kont. Dotychczasowe doświadczenia pokazały, że platformy te nie wywiązują się w pełni z kodeksowych zobowiązań, co może oznaczać konieczność podjęcia przez Komisję Europejską bardziej restrykcyjnych środków regulacyjnych.

[18] S. Stolton, *EU mulls disinformation regulation but admits alert system has 'never been triggered'*, Euractiv, 29.10.2019, www.euractiv.com.

[19] G. Gotev, *Experts lament underfunding of EU task force countering Russian disinformation*, Euractiv, 23.11.2018, www.euractiv.com; interpelacja Anny Fotygi w sprawie poszerzenia zakresu prac i wzmocnienia grupy zadaniowej East Stratcom oraz konieczności przekształcenia jej w pełnoprawną stałą strukturę w ramach ESDZ, Parlament Europejski, 6.04.2020, www.europarl.europa.eu.