**Informacja wprowadzająca**

**Sesja I: Ochrona i bezpieczeństwo Unii Europejskiej. Zagrożenia hybrydowe jako zewnętrzny czynnik destabilizujący Europę**

**Wprowadzenie**

Unia Europejska jest szczególnego rodzaju organizacją. Jest to struktura ponadnarodowa niepodobna do żadnej innej ani współczesnej, ani historycznej, oparta na wartościach, w tym m.in. demokracji, praworządności, tolerancji, pluralizmie, poszanowaniu praw człowieka. Unijne wartości są podstawą dla zasad i instytucji, pośród których znajdują się lojalna współpraca, poszanowanie podstawowych struktur politycznych i konstytucyjnych poszczególnych państw członkowskich, wolny rynek, współpraca, dialog i konsensus. Organizacja, oparta na wartościach, zasadach i ideałach, jest szczególnie podatna na różne formy destabilizacji i zagrożeń. Dlatego tak ważne są mechanizmy zabezpieczające ją przed destabilizacją, osłabieniem aksjologicznej atrakcyjności i wewnętrznej spójności oraz zdolności do aktywnego działania i odpierania zagrożeń.

Budowanie odporności jest kluczowym zadaniem UE. Poza pełnoskalowym konfliktem zbrojnym w Ukrainie, UE zmaga się z wieloma innymi, mniej oczywistymi zagrożeniami. Narażają one jedność Unii Europejskiej i jej zdolność do działania, a w niektórych przypadkach kwestionują również jej pryncypia, i zawsze – co w praktyce jest najgroźniejsze – erodują społeczne zaufanie poprzez stawianie znaku równości między moralnością a siłą, definiowaną jako witalność, skuteczne działanie, odporność na zagrożenia i wyzwania.

Pole działań hybrydowych jest niemal nieograniczone. Może to być m.in. przestrzeń polityczna, dyplomatyczna, dezinformacyjno-propagandowa, gospodarcza, kulturalna, społeczna, militarna oraz humanitarna. Zagrożenia hybrydowe są różnorodne i ciągle się zmieniają. Takie działania mogą prowadzić zarówno agenci służb specjalnych obcego państwa i osoby z nimi współpracujące, jak również - świadomie bądź nie - organizacje, stowarzyszenia, instytucje, partie polityczne, firmy, korporacje czy np. celebryci. Należy przy tym podkreślić, że działania hybrydowe mają zwykle charakter utrudniający ich jednoznaczne zakwalifikowanie i przypisanie odpowiedzialności sprawcom. Powoduje to trudność w ich początkowym rozpoznaniu i zdefiniowaniu.

**Bieżące wydarzenia**

W 2016 r. Unia Europejska we „Wspólnych ramach dotyczących przeciwdziałania zagrożeniom hybrydowym" zdefiniowała zagrożenia hybrydowe jako *„kombinację represyjnych i wywrotowych działań, wykorzystujących konwencjonalne i niekonwencjonalne*

*metody (tj. dyplomatyczne, militarne, ekonomiczne i technologiczne), które mogą być stosowane w sposób skoordynowany przez podmioty państwowe i niepaństwowe, by osiągnąć określone cele, przy czym działania te są poniżej progu oficjalnie wypowiedzianej wojny".* Mogą być one wykorzystywane do realizacji różnych celów strategicznych, operacyjnych i taktycznych, których wspólnym mianownikiem jest destabilizowanie państw członkowskich i całej Wspólnoty, a także ingerowanie w ich procesy polityczne, społeczne i gospodarcze.

Elastyczne podejście Unii do tego zagadnienia wynika ze specyfiki samego zjawiska, które jest złożone, wieloaspektowe i niejednoznaczne, a także odzwierciedla różne perspektywy bezpieczeństwa i priorytety polityki zagranicznej poszczególnych państw członkowskich. Takie podejście pozwala uwzględnić zarówno zagrożenia z kierunku wschodniego (Rosja, Białoruś) i południowego (Iran, organizacje terrorystyczne, nieregularna migracja), jak i o zasięgu globalnym (Chiny). Katalog metod i taktyk hybrydowych obejmuje m.in. działania dezinformacyjne i propagandowe, cyberataki, ingerencje w procesy polityczne (np. wybory i referenda), presję gospodarczą, instrumentalizację nieregularnej migracji, wspieranie przez państwa grup zbrojnych i zatrudnianie najemników, operacje wywiadowcze o charakterze dywersyjno-sabotażowym, działalność terrorystyczną czy użycie środków chemicznych, biologicznych, radiologicznych i jądrowych (CBRJ). Od 2015 r. UE doświadcza wrogiej aktywności hybrydowej przede wszystkim ze strony Rosji. W mniejszym stopniu – lecz z wyraźną tendencją wzrostową – tego rodzaju metody są stosowane także przez Białoruś, Iran i Koreę Północną oraz organizacje terrorystyczne i środowiska radykalne.

Metody hybrydowe mogą być wykorzystywane w różnym zakresie i ze zmienną intensywnością, mogą być także dowolnie łączone przez państwowych lub pozapaństwowych agresorów, których sposób działania nie jest jednakowy. Co więcej, katalog narzędzi walki hybrydowej ma charakter otwarty. W ocenie unijnych instytucji do jego rozszerzenia prowadzi m.in. nasilająca się rywalizacja polityczna z udziałem Rosji (zwłaszcza po inwazji na Ukrainę) i Chin, niestabilna sytuacja w sąsiedztwie UE oraz tzw. weaponizacja kolejnych sektorów (np. ochrony zdrowia, klimatu i środowiska).

Od 2016 r. UE rozwija zdolności przeciwdziałania zagrożeniom hybrydowym w czterech obszarach: 1) świadomość sytuacyjna, 2) budowa odporności, 3) przeciwdziałanie kryzysom i zarządzanie kryzysowe, 4) współpraca międzynarodowa (zwłaszcza z NATO). W Kompasie Strategicznym UE postuluje się wzmocnienie tych zdolności w ramach skoordynowanej reakcji Unii na kryzysy wywołane metodami hybrydowymi, a przede wszystkim – stworzenie nowych mechanizmów oraz usprawnienie ich wykorzystywania. Ciężar odpowiedzialności za zwalczanie zagrożeń hybrydowych spoczywa obecnie (zgodnie z art. 4 ust. 2 TUE)na krajowych instytucjach bezpieczeństwa (tj. służbach specjalnych, policji i wojsku), które mają do tego odpowiednie umocowanie prawne i kompetencje wykonawcze. Kompas Strategiczny nie

dokonuje zmian w tym obszarze. Instrumentarium tworzone w ramach EU Hybrid Toolbox, by osiągnąć efekt synergii i skuteczniej reagować, ma natomiast w większym stopniu wspierać krajowe wysiłki na rzecz zwalczania zagrożeń hybrydowych oraz koordynować wspólne działania państw członkowskich.

Budowa odporności państw Unii i ich społeczeństw jest ukierunkowana na zmniejszenie podatności na wrogą dezinformację i propagandę oraz na wzmocnienie ochrony infrastruktury krytycznej przed cyberatakami, terroryzmem, dywersją i sabotażem. Kompas Strategiczny szczególną uwagę przypisuje wzmocnieniu odporności UE na zagraniczne manipulacje informacyjne i ingerencje w procesy polityczne.

Podejście UE do zwalczania manipulacji informacyjnych składa się z czterech elementów przyjętych przez Komisję Europejską w grudniu 2018 r. w Planie działania na rzecz zwalczania dezinformacji (*The Action Plan against Disinformation*): 1) zwiększenie zdolności instytucji UE do wykrywania, analizowania i ujawniania dezinformacji; 2) wzmocnienie skoordynowanych i wspólnych reakcji na dezinformację; 3) mobilizowanie sektora prywatnego do zwalczania dezinformacji oraz 4) podnoszenie świadomości i poprawa odporności społecznej poprzez wspieranie niezależnego dziennikarstwa, inicjatywy weryfikowania faktów (*fact-checking*) i promowanie edukacji medialnej.

W odpowiedzi na rosyjskie kampanie dezinformacyjno-psychologiczne w ramach Europejskiej Służby Działań Zewnętrznych powołano w 2015 r. grupę zadaniową *East StratCom*, która miała być odpowiedzialna za monitorowanie, analizę i reagowanie na rosyjską propagandę i dezinformację. Początkowo zespół liczył zaledwie trzy osoby, obecnie dysponuje 16 pełnoetatowymi pracownikami, co najlepiej świadczy o znaczeniu tej jednostki w UE. *East StratCom* monitoruje przekazy informacyjne publikowane w ponad 20 językach. Zespół zidentyfikował kilkadziesiąt tysięcy przypadków rosyjskiej dezinformacji, które zostały skatalogowane w bazie *EUvsDisinfo*. Zespół prowadzi także szkolenia dla personelu państw partnerskich, podejmuje działania na rzecz wzmocnienia niezależnego dziennikarstwa oraz promuje wiedzę o UE i jej polityce w państwach Partnerstwa Wschodniego. Podobne zadania realizują utworzone w 2017 r. analogiczne zespoły (sześciu pełnoetatowych pracowników każdy) odpowiedzialne za region Bałkanów Zachodnich (*Western Balkans Task Force*) oraz Bliski Wschód i Afrykę Północną (*South Stratcom Task Force*), które koncentrują się na przeciwdziałaniu radykalizacji, zwalczaniu propagandy organizacji terrorystycznych, a także dezinformacji ze strony m.in. Rosji i Iranu. Wszystkie te zespoły wchodzą w skład Wydziału Komunikacji Strategicznej, Grup Zadaniowych i Analiz Informacyjnych Europejskiej Służby Działań Zewnętrznych, który wspiera instytucje UE w zakresie planowania polityk, strategii i narzędzi komunikacji strategicznej. Zapewnia także wsparcie (np. analizy i instrukcje zwalczania dezinformacji) placówkom dyplomatycznym UE, misjom i operacjom wspólnej polityki bezpieczeństwa i obrony (WPBiO). Wydział rozwija także współpracę z państwami

partnerskimi, G7, organizacjami pozarządowym, społeczeństwem obywatelskim i sektorem prywatnym (np. w zakresie pozyskiwania danych przy wykorzystaniu nowoczesnych oprogramowań i technologii). Celem tych działań jest budowa świadomości społecznej i wzmacnianie odporności państw na dezinformację w sąsiedztwie UE.

Współpraca między Unią Europejską a NATO w zakresie komunikacji strategicznej ma na celu zapewnienie efektywnego przekazu oraz wspólnych działań w odpowiedzi na wyzwania związane z bezpieczeństwem. Jednym z przykładów tej współpracy jest współdziałanie jednostki East StratCom UE z NATO Strategic Communications Centre of Excellence (NATO StratCom COE), które ma swoją siedzibę w Rydze. Główne cele tej kooperacji to wymiana doświadczeń i najlepszych praktyk, co umożliwia wzajemne uzupełnianie się w zakresie analizy i przeciwdziałania dezinformacji. Dodatkowo, koordynacja działań w obszarze komunikacji strategicznej i cyberbezpieczeństwa pozwala na osiągnięcie efektu synergii. Tego typu współpraca jest kluczowa w złożonym i dynamicznie zmieniającym się środowisku geopolitycznym.

Budowa odporności państw UE dotyczy także kluczowych sektorów, takich jak bezpieczeństwo cybernetyczne, infrastruktura krytyczna, energetyka, transport, obronność, system finansowy, bezpieczeństwo morskie czy przestrzeń kosmiczna. Wysiłek ten jest zorientowany przede wszystkim na tworzenie instrumentów prawnych oraz zdolności do reagowania na incydenty i sytuacje kryzysowe wywołane metodami hybrydowymi (zwłaszcza w cyberprzestrzeni). Przełomem w podejściu UE do cyberbezpieczeństwa było przyjęcie w 2016 r. dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych (tzw. dyrektywa NIS). Obliguje ona państwa członkowskie do zagwarantowania minimalnych wspólnych standardów cyberbezpieczeństwa, m.in. dzięki przyjęciu narodowych strategii bezpieczeństwa cybernetycznego czy utworzeniu zespołów reagowania na incydenty komputerowe, które będą działać w ramach europejskiej sieci CERT. Unia nałożyła także obowiązek składania raportów o cyberincydentach na kluczowych usługodawców z sektora energetycznego, transportu, bankowości i finansów, służby zdrowia, zaopatrzenia w wodę czy infrastruktury cyfrowej. UE za pośrednictwem Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) i Europejskiej Organizacji ds. Cyberbezpieczeństwa (ECSO) wspiera także – poza regulacyjną – działalność badawczą i współpracę publiczno-prywatną. Zdolności państw członkowskich w zakresie cyberobrony są z kolei rozwijane w ramach czterech projektów współpracy strukturalnej PESCO, które dotyczą wymiany informacji o cyberincydentach, koordynacji działań, wsparcia i wspólnej odpowiedzi, a także badań i szkolenia. W grudniu 2020 r. Unia przyjęła nową strategię cyberbezpieczeństwa, która ma zwiększyć odporność państw członkowskich na cyberataki oraz lepiej chronić przed nimi infrastrukturę krytyczną. Przykładem sektorowego działania w tym obszarze jest zestaw narzędzi unijnej cyberdyplomacji mający odstraszać potencjalnych cyberagresorów (EU Cyber Diplomacy Toolbox). W maju 2019 r. w jego ramach utworzono reżim

sankcyjny, który ma być odpowiedzią na cyberataki dokonywane spoza UE na państwa członkowskie lub wykorzystujące infrastrukturę znajdującą się poza granicami Wspólnoty. Wpisane na „czarną listę" podmioty odpowiedzialne lub wspierające cyberataki przeciwko państwom UE zostaną objęte sankcjami w postaci zakazu wjazdu na terytorium UE lub zamrożeniem aktywów. Podobny reżim sankcyjny wprowadzono wobec państw stosujących broń chemiczną (niejawna lista zawiera 20 substancji), co jest bezpośrednią odpowiedzią UE na użycie przez rosyjskie służby specjalne gazu paralityczno-drgawkowego nowiczok na terytorium Wielkiej Brytanii. W latach 2019–2022 UE udzieliła także wsparcia finansowego w łącznej wysokości 11,6 mln euro Organizacji ds. Zakazu Broni Chemicznej (OPCW) na prace związane z przeciwdziałaniem rozwojowi broni chemicznej i jej użyciu.

**Wyzwania**

Wyzwania związane z budowaniem odporności UE i jej państw członkowskich wyznacza przede wszystkim hybrydowość działań świadomie i celowo podejmowanych przez podmioty, którym z różnych powodów zależy na demontowaniu spójności działań Unii. Charakterystyka zagrożeń hybrydowych, a przede wszystkim to, że są one wielokierunkowe, prowadzone w sposób skryty przy zastosowaniu różnych środków, a na dodatek mocno zmienne w czasie, jest kluczowym wyzwaniem dla UE.

Wyzwaniem obserwowanym od dłuższego już czasu jest złożoność zagrożeń hybrydowych. Choć UE identyfikuje pewien katalog metod walki hybrydowej, ich pełna klasyfikacja pozostaje trudna ze względu na ich zmienność i wieloaspektowość. Drugim kluczowym wyzwaniem jest przewidywane zwiększenie liczby sektorów podatnych na tzw. weaponizację (m.in. bezpieczeństwo energetyczne, zdrowotne, informacyjne, zmiany klimatyczne, ochronę środowiska czy nowe technologie związane ze sztuczną inteligencją). To oznacza, że rośnie liczba tzw. sektorów strategicznych, które mogą być przynajmniej potencjalnym polem działań hybrydowych. Co więcej, rejon Morza Bałtyckiego jest dobrą ilustracją tego, jak bardzo działania hybrydowe są wielokierunkowe i groźne. Bałtyk potwierdza, że aktywnością hybrydową ze strony Rosji są: tzw. flota cieni, sabotaż sieci telekomunikacyjnej, zakłócanie sygnału GPS czy zagrożenia ekologiczne.

Unijne podejście do zwalczania zagrożeń hybrydowych koncentruje się jedynie na ich pozamilitarnym wymiarze (tj. dezinformacji, propagandzie, cyberatakach), w niewystarczającym stopniu rozwijając militarne zdolności do odpowiedzi w przypadku zastosowania pełnego spektrum metod hybrydowych (w tym wojskowych lub paramilitarnych). Z tego też powodu Unia powinna zastanowić się, jaka mogłaby być rola sił szybkiego reagowania (*Rapid Deployment Capacity*) podczas kryzysu hybrydowego na terytorium państw członkowskich, co byłoby wyraźnym sygnałem dla agresora, że dalsza

eskalacja sytuacji spotka się ze zdecydowaną odpowiedzią Unii. Działania te powinny być podejmowane w porozumieniu z NATO, na zasadzie komplementarności obu organizacji, a jednocześnie powinny wzmacniać europejski filar Sojuszu.

Ponadto wydaje się, że ważnym wyzwaniem dla Unii jest bardziej odważne sięganie po instrumenty już istniejące. UE powinna jednoznacznie określić warunki użycia klauzuli solidarności lub klauzuli wzajemnej pomocy. Zwiększyłoby to bezpieczeństwo państw członkowskich, które mogłyby liczyć na jednoczesne i spójne działanie i Unii, i NATO (tym bardziej, że w zwalczaniu zagrożeń hybrydowych UE wprost deklaruje ścisłą współpracę z NATO). Niejednoznaczność działań hybrydowych stwarza ryzyko rozbieżnej interpretacji sytuacji kryzysowej, wydłużenia procesów decyzyjnych w UE, a tym samym spowolnienia lub nieadekwatności reakcji. Zminimalizować je można m.in. poprzez wypracowanie rozwiązań w drodze symulacji i ćwiczeń prowadzonych zarówno w ramach UE, jak i we współpracy z NATO, opierających się na rzeczywistych scenariuszach kryzysów hybrydowych. Powinny one także uwzględniać możliwe przyszłe formy ataków z wykorzystaniem nowych metod i taktyk.

**Punkty do dyskusji**

1. Czy UE może skutecznie przeciwdziałać zagrożeniom hybrydowym, zamiast działać reaktywnie?
2. Jak skutecznie zwalczać dezinformację i propagandę, nie naruszając wolności słowa i pluralizmu?
3. Jak skutecznie informować społeczeństwo o zagrożeniach hybrydowych?
4. Czy istniejące narzędzia UE są wystarczające do zwalczania zagrożeń hybrydowych, czy potrzebne są nowe rozwiązania?
5. W jaki sposób sztuczna inteligencja może zostać wykorzystana do destabilizacji UE i jak się przed tym bronić?
6. Jak chronić kluczowe elementy systemu demokratycznego przed ingerencją zewnętrzną?
7. Jak utrzymać demokrację i praworządność, jednocześnie wzmacniając odporność UE?