POLITICILE UNIUNII EUROPENE PENTRU DEZVOLTAREA CAPACITĂȚILOR DE CONTRACARARE A AMENINȚĂRILOR HIBRIDE

Colonel Marian ȘTEFAN
Expert, Ministerul Apărării Naționale
DOI: 10.55535/GMR.2023.1.9

Combaterea amenințărilor hibride reprezintă una dintre principalele dimensiuni ale politicilor Uniunii Europene exprimate în documentul elaborat anul trecut, denumit „Busola strategică” („A Strategic Compass for Security and Defence”), care ghidează dezvoltarea capabilităților Uniunii în domeniul securității internaționale. Noul document presupune combinarea instrumentelor dezvoltate începând cu 2016 pentru combaterea amenințărilor hibride într-un „Set de instrumente al UE” („EU Hybrid Toolbox”), care va include, de asemenea, noi instrumente și moduri de acțiune.

În timp ce responsabilitatea principală pentru combaterea activității hibride ostile va continua să revină statelor membre, Uniunea Europeană își propune să dețină o capacitate mai mare de sprijin și coordonare pentru a preveni și a răspunde adecvat noilor amenințări. Abordarea Uniunii Europene se concentrează pe aspecte non-militare și pe dezvoltarea capabilităților militare de răspuns la crize hibride, aspect ce presupune creșterea importanței cooperării cu NATO în acest domeniu.

Cuvinte-cheie: Uniunea Europeană, amenințări hibride, politici, instrumente, reziliență.

ASPECTE GENERALE PRIVIND NOUA PARADIGMĂ DE SECURITATE EUROPEANĂ

Trăind într-o eră a concurenței strategice și a amenințărilor complexe de securitate ce presupun revenirea războiului în Europa, odată cu agresiunea nejustificată și neprovocată a Rusiei împotriva Ucrainei, precum și pe marginea actualelor schimbări geopolitice majore generate de ambițiile Chinei, se ridică o serie de provocări cu privire la capacitatea Uniunii Europene și, implicit, a statelor membre de a-și promova viziunea și de a-și apăra interesele. Confruntându-ne, la granițele UE și dincolo de acestea, cu conflicte, agresiuni militare și surse de instabilitate ce duc la suferințe umanitare și dislocări forțate a milioane de oameni, constatăm că amenințările hibride au crescut atât ca frecvență, cât și ca impact. Competiția și ambițiile politice ale unor state generează încercări tot mai mari de constrângere economică și energetică, iar conflictele și instabilitatea sunt adesea agravate de efectul multiplicator al schimbărilor climatice.

Toate aceste aspecte conduc spre un peisaj general de securitate ce a devenit, mai mult ca oricând, volatil, complex și fragmentat, din cauza amenințărilor hibride ce presupun instrumentarea cumulată a unor metode coercitive. Dinamica instabilității locale și regionale, care se hrănește cu guvernanță disfuncțională și contestație a valorilor democratice, existentă în vecinătatea noastră, uneori alimentată de inegalități, tensiuni religioase și etnice, este din ce în ce mai impactată de efectele amenințărilor neconvenționale și transnaționale și de rivalitatea geopolitică de putere. Acest lucru erodează capacitatea sistemului multilateral al Uniunii Europene de a preveni și a atenua riscurile și crizele.

Începând cu anul 2016, UE și-a mobilizat resursele și a creat noi instrumente pentru combaterea amenințărilor hibride. Aceste acțiuni reprezintă, în primul rând, răspunsul Uniunii Europene la activitățile destabilizatoare ale Rusiei și Chinei, precum și ale unor state mai mici,

Confruntându-ne, la granițele UE și dincolo de acestea, cu conflicte, agresiuni militare și surse de instabilitate ce duc la suferințe umanitare și dislocări forțate a milioane de oameni, constatăm că amenințările hibride au crescut atât ca frecvență, cât și ca impact. Competiția și ambițiile politice ale unor state generează încercări tot mai mari de constrângere economică și energetică, iar conflictele și instabilitatea sunt adesea agravate de efectul multiplicator al schimbărilor climatice.

precum Belarus, Iran sau Coreea de Nord, dar și a activităților desfășurate de entități non-statale, precum organizații teroriste și grupuri extremiste. Până în prezent, eforturile UE s-au concentrat pe combaterea dezinformarii și a propagandei și pe consolidarea protecției infrastructurii critice împotriva atacurilor cibernetice. În actuala *„Busolă strategică”*, adoptată de Consiliul UE la 21 martie 2022, la mai puțin de o lună de la invazia rusă în Ucraina, accentul se pune pe creșterea rezilienței statelor și societăților în fața manipulării informațiilor și interferența în procesele politice, precum și pe extinderea capacității UE de a sprijini statele membre în răspunsul la crizele cauzate de metodele, tehnicile și tacticile hibride. Acesta este scopul unui nou set de instrumente de răspuns și reacție, denumit *„EU Hybrid Toolbox”*.

În actuala „Busolă strategică”, adoptată de Consiliul UE la 21 martie 2022, accentul se pune pe creșterea rezilienței statelor și societăților în fața manipulării informațiilor și interferența în procesele politice, precum și pe extinderea capacității UE de a sprijini statele membre în răspunsul la crizele cauzate de metodele, tehnicile și tacticile hibride.

Prezentul studiu își propune definirea problemelor actuale cu care societatea europeană se confruntă, identificarea cauzei acestor probleme de securitate care generează o serie de amenințări la adresa stabilității politice, economice, sociale, informaționale și militare și analizarea și prezentarea succintă a măsurilor pe care UE le-a adoptat, de-a lungul anilor, pentru a găsi o formulă adaptată de răspuns în cheia unui concept denumit reziliență.

ABORDAREA EUROPEANĂ PRIVIND COMBATEREA AMENINȚĂRILOR HIBRIDE

În 2016, în documentul denumit *„Cadrul comun pentru combaterea amenințărilor hibride”*, UE a definit amenințările respective ca fiind un *„amestec de activități coercitive și subversive, metode convenționale și neconvenționale (diplomatice, militare, economice, tehnologice), care pot fi utilizate în mod coordonat de către actori statali sau non-statali pentru a atinge obiective specifice, situându-se, în același timp, sub pragul războiului declarat oficial”* (Comisia Europeană, 2016). Aceste tipuri de activități pot fi utilizate pentru a urmări o varietate de obiective strategice, operaționale și tactice cu numitorul comun al destabilizarii statelor și al interferării în procesele lor politice, sociale și economice, afectând atât statele membre, cât și comunitatea, în ansamblu. Abordarea amplă a UE față de această problemă derivă din specificul fenomenului în sine, în special din complexitatea acțiunilor

hibride, natura complexă a acestora și ambiguitate. Răspunsul reflectă, de asemenea, diferitele perspective de securitate și prioritățile de politică externă ale statelor membre. Această abordare flexibilă face posibilă luarea în considerare atât a amenințărilor din est (Rusia, Belarus), din sud (Iran, organizații teroriste, migrație ilegală în masă), cât și a celor cu acoperire globală (China).

Catalogul metodelor și tacticilor hibride include activități de dezinformare și propagandă, atacuri cibernetice, interferențe în procesele politice (de exemplu, alegeri și referendumuri), presiune economică, instrumentarea migrației neregulate, sprijinirea de către stat a grupurilor armate și angajarea mercenarilor, operații informaționale cu caracter subversiv, activități de natură teroristă sau utilizarea agenților chimici, biologici, radiologici și nucleari (CBRN). Metodele hibride pot fi utilizate în diferite măsuri și intensități și pot fi combinate liber de către agresori statali sau non-statali, al căror *modus operandi* nu este același. În plus, catalogul instrumentelor hibride de război este *„deschis”* oricăror acțiuni ce pot produce efecte perturbatoare la nivel societal. În opinia instituțiilor UE, rivalitățile politice tot mai mari cu Federația Rusă (în special, după invazia Ucrainei) și China, situația instabilă din vecinătatea UE, militarizarea unor sectoare vitale (de exemplu, problemele de securitate legate de sănătate), aspectele legate de mediul înconjurător și accesul la resurse pot constitui factori de risc la adresa securității spațiului comunitar. Acest lucru este exemplificat de campaniile rusești și chineze de dezinformare privind vaccinarea în timpul pandemiei de COVID-19. În mod similar, probleme precum cele legate de protecția mediului pot fi folosite pentru a crea polarizare socială și diviziuni în cadrul UE. Schimbările climatice, la rândul lor, pot contribui la destabilizarea vecinătății sudice a Uniunii, la crizele migrației și la apariția organizațiilor teroriste. Instrumentarea acestor fenomene de către actori externi (de exemplu, crearea de rute pentru introducerea ilegală de migranți sau sprijinul unor formațiuni sau grupări radicale pentru a comite atacuri teroriste) reprezintă o amenințare directă pentru statele membre ale UE. Catalogul amenințărilor hibride este, de asemenea, extins de tehnologiile emergente și perturbatoare (EDT), inclusiv dezvoltarea inteligenței artificiale, oferind capacități tehnice

Catalogul metodelor și tacticilor hibride include activități de dezinformare și propagandă, atacuri cibernetice, interferențe în procesele politice, presiune economică, instrumentarea migrației neregulate, sprijinirea de către stat a grupurilor armate și angajarea mercenarilor, operații informaționale cu caracter subversiv, activități de natură teroristă sau utilizarea agenților chimici, biologici, radiologici și nucleari.

avansate pentru campanii de dezinformare și propagandă, precum și activități de culegere de informații și subversiune. Aceste considerații fac mult mai dificilă dezvoltarea procedurilor de răspuns la diferite scenarii de atac hibrid, care, ca urmare a naturii transfrontaliere și în rețea a amenințărilor hibride, necesită o abordare cuprinzătoare și multidimensională a detectării, avertizării timpurii, contracarării și răspunsului de urgență.

Sarcina responsabilității pentru combaterea amenințărilor hibride revine instituțiilor de securitate națională, care au autoritatea legală și puterile executive pentru a face acest lucru. Busola strategică nu face modificări în acest domeniu, în schimb, instrumentele dezvoltate în cadrul UE Hybrid Toolbox sunt menite să ofere un sprijin mai mare eforturilor naționale de combatere a amenințărilor hibride și să coordoneze acțiunile comune ale statelor membre pentru a obține sinergii și un răspuns mult mai eficient.

Din 2016, UE și-a propus dezvoltarea capabilităților de contracarare a amenințărilor hibride pornind de la patru domenii esențiale: (1) conștientizarea situației; (2) construirea și aplicarea politicilor de reziliență; (3) contracararea și răspunsul la crize (inclusiv depășirea efectelor acestora); și (4) cooperarea și coordonarea cu partenerii și organizațiile internaționale (în principal, NATO). În acest sens, actualul *„Strategic Compass”* solicită consolidarea acestor domenii prin crearea de noi mecanisme și îmbunătățirea utilizării acestora ca parte a răspunsului coordonat al Uniunii la crizele hibride. Într-adevăr, sarcina responsabilității pentru combaterea amenințărilor hibride revine instituțiilor de securitate națională (de exemplu, structuri de informații, servicii de securitate, poliție și armată), care au autoritatea legală și puterile executive pentru a face acest lucru [în conformitate cu articolul 4 alineatul (2) din Tratatul privind UE/TUE]. Busola strategică nu face modificări în acest domeniu, în schimb, instrumentele dezvoltate în cadrul UE Hybrid Toolbox sunt menite să ofere un sprijin mai mare eforturilor naționale de combatere a amenințărilor hibride și să coordoneze acțiunile comune ale statelor membre pentru a obține sinergii și un răspuns mult mai eficient.

IMPORTANȚA ACȚIUNILOR COMUNE

Busola strategică subliniază importanța continuării consolidării capabilităților de intelligence ale UE pentru a oferi cunoașterea situației și capacități de prognozare a amenințărilor. Crearea mecanismelor de partajare a informațiilor privind amenințările hibride prezintă o importanță deosebită pentru a identifica, în primul rând, un *modus operandi* al serviciilor de informații străine care instrumentează astfel de acțiuni. Îmbunătățirea gradului de conștientizare a instituțiilor UE și a statelor membre în acest domeniu va spori capacitatea Uniunii

de a detecta și de a răspunde într-o manieră promptă și adaptată crizelor cauzate de metodele hibride ale vectorilor ostili. De asemenea, va îmbunătăți coordonarea acțiunilor întreprinse de statele membre la nivel individual. Activitățile în acest domeniu au fost inițiate în 2016, odată cu crearea Celulei de fuziune hibridă (Hybrid Fusion Cell) din cadrul Centrului de Informații al UE (EU Intelligence and Situation Centre – EU INTCENT). Aceasta este alcătuită din analiști civili și militari (de la Direcția de informații din cadrul Statului Major al UE/EUMS) responsabili cu producerea de rapoarte, briefinguri și analize în cadrul Capacității unice de analiză a informațiilor (Single Intelligence Analysis Capacity/SIAC) privind amenințările hibride care sunt identificate la nivelul țărilor membre ale UE și în vecinătatea sa. Studiile sunt realizate pe baza informațiilor din surse deschise și clasificate, furnizate de serviciile de informații și de securitate ale statelor membre, agențiile UE (de exemplu, Centrul european pentru criminalitate cibernetică, Centrul european de combatere a terorismului sau Frontex) și țările partenere (de exemplu, SUA, Canada, Norvegia). În ceea ce privește informațiile privind amenințările cibernetice, activitatea Celulei de fuziune hibridă este susținută de reprezentanți ai Echipei de răspuns la urgențe informatice pentru instituțiile UE (CERT-EU). Schimbul de informații sensibile privind, de exemplu, detaliile tehnice ale conturilor, administratorilor, software-ului sau infrastructurii utilizate pentru a efectua o operațiune de dezinformare este crucial pentru a putea atribui responsabilitatea acestor acțiuni unei anumite entități și pentru a impune sancțiuni asupra acesteia (Kaca, 2021).

Celula de fuziune hibridă este instituția principală responsabilă cu furnizarea de cunoaștere a situației pentru instituțiile UE și statele membre. Crearea sa a contribuit la sporirea capacității Uniunii de a detecta crizele induse de amenințările hibride într-un stadiu incipient, precum și la accelerarea și coordonarea răspunsului comun al statelor membre.

Celula de fuziune hibridă este instituția principală responsabilă cu furnizarea de cunoaștere a situației pentru instituțiile UE și statele membre. Crearea sa a contribuit la sporirea capacității Uniunii de a detecta crizele induse de amenințările hibride într-un stadiu incipient, precum și la accelerarea și coordonarea răspunsului comun al statelor membre. Un exemplu în acest sens este răspunsul UE (inclusiv sub forma unei comunicări strategice eficiente) la criza migrației susținute de Belarus, declanșată la jumătatea anului 2021 (cu sprijinul Federației Ruse), care a durat câteva luni la granițele cu Polonia, Lituania și Letonia (Dyner, 2022). În ciuda activităților de dezinformare bieloruso-ruse menite să creeze perturbări cu privire la interpretarea și înțelegerea

situației de la graniță, UE a rămas consecventă și a considerat aceasta un atac de tip hibrid (Consiliul Europei, 2021).

Pentru a crește gradul de conștientizare a situației cu privire la manipularea informațiilor ostile, în martie 2019, UE a instituit Sistemul de alertă rapidă privind dezinformarea. Schimbul de informații în cadrul acestui sistem are loc prin intermediul punctelor de contact stabilite în fiecare țară din Uniune. Sistemul a fost utilizat în 2020, în timpul pandemiei COVID-19, când spațiul informațional a fost inundat de un val de dezinformare rusă și chineză, subminând încrederea în vaccinurile occidentale, în instituțiile UE și în strategiile de vaccinare și alimentând mișcările și protestele privind anti-vaccinarea (Ștefan, 2020). Ținta principală a atacurilor mediatice de la acea vreme era Agenția Europeană pentru Medicamente. Sistemul a fost folosit pentru a face schimb de informații între instituțiile UE și statele membre, reprezentanții sectorului privat și membrii G7 și NATO. Cu toate aceste mecanisme și acțiuni coordonate pentru combaterea dezinformării, valul de teorii ale conspirației răspândite de canalele de știri pro-Rusia și pro-China (inclusiv *„fabricile de troli”*) a generat perturbări de percepție și neîncredere în rândul opiniei publice.

Pentru a crește gradul de conștientizare a situației cu privire la manipularea informațiilor ostile, în martie 2019, UE a instituit Sistemul de alertă rapidă privind dezinformarea. Schimbul de informații în cadrul acestui sistem are loc prin intermediul punctelor de contact stabilite în fiecare țară din Uniune.

CONSTRUIREA POLITICILOR ȘI MECANISMELOR DE REZILIENȚĂ

Consolidarea rezilienței statelor membre ale UE și a societăților are ca scop reducerea vulnerabilității acestora la dezinformarea și propaganda unor entități ostile, precum și dezvoltarea protecției infrastructurii critice împotriva atacurilor cibernetice, terorismului, subversiunii și sabotajului. *Busola strategică* acordă o atenție deosebită consolidării rezilienței UE împotriva manipulării informațiilor și a interferenței în procesele politice. Abordarea UE pentru combaterea manipulării informațiilor constă în patru elemente adoptate de Consiliul European în decembrie 2018 în *„Planul de acțiune împotriva dezinformarii”* și vizează: creșterea capacității instituțiilor UE de a detecta, analiza și expune dezinformarea, consolidarea răspunsurilor coordonate și colective la dezinformare, mobilizarea sectorului privat pentru combaterea dezinformarii și creșterea gradului de conștientizare și îmbunătățirea rezilienței publice prin sprijinirea jurnalismului

independent, inițiative de verificare a faptelor și promovarea educației media.

În 2015, ca răspuns la operațiile informaționale și psihologice derulate de Federația Rusă pentru a masca acțiunile desfășurate în Ucraina și în alte zone și domenii de interes strategic, la nivelul UE a fost înființat grupul operativ East StratCom în cadrul Serviciului European pentru Acțiuni Externe (SEAE), pentru a monitoriza, analiza și răspunde campaniilor rusești de propagandă și dezinformare încadrate în spectrul amenințărilor hibride. East StratCom monitorizează, în prezent, mesajele informative publicate în peste 20 de limbi. Până la jumătatea lunii mai 2022, echipa identificase aproape 14.000 de cazuri de dezinformare rusă și le catalogase în baza de date EUvsDisinfo. În plus, echipa desfășoară cursuri de formare pentru personalul țărilor partenere, precum și activități în scopul consolidării jurnalismului independent, promovând conștientizarea UE și politicile acesteia în țările Parteneriatului Estic. Sarcini similare sunt îndeplinite de echipe înființate în 2017, responsabile pentru regiunea Balcanilor de Vest (Western Balkans Task Force) și regiunea Orientului Mijlociu și Africa de Nord (South Stratcom Task Force), concentrându-se pe combaterea radicalizării, a propagandei organizațiilor teroriste și dezinformarea din Rusia, China, Iran sau Turcia. Toate cele trei echipe fac parte din Divizia de comunicare strategică, grupuri operative și analiză a informațiilor a SEAE (SG.STRAT.2), care sprijină instituțiile UE în planificarea politicilor, strategiilor și instrumentelor de comunicare strategică. De asemenea, oferă sprijin (de exemplu, sub formă de analiză și instrucțiuni privind modul de combatere a dezinformării) misiunilor, operațiilor și misiunilor diplomatice ale UE în cadrul Politicii comune de securitate și apărare (PSAC), dezvoltând, de asemenea, cooperarea cu țările partenere, G7, ONG-uri, societatea civilă și sectorul privat (de exemplu, cu privire la achiziția de date folosind software și tehnologie modernă). Scopul acestor activități este de a crește gradul de conștientizare a publicului și de a întări reziliența țărilor la dezinformare în vecinătatea UE .

Potrivit SEAE, dezinformarea rusă reprezintă cea mai mare amenințare pentru statele membre ale UE din cauza naturii sale sistemice. Rusia are resursele necesare pentru a desfășura campanii de dezinformare ca parte a unei strategii pe termen lung de destabilizare

GÂNDIREA MILITARĂ ROMÂNEASCĂ

În 2015, ca răspuns la operațiile informaționale și psihologice derulate de Federația Rusă pentru a masca acțiunile desfășurate în Ucraina și în alte zone și domenii de interes strategic, la nivelul UE a fost înființat grupul operativ East StratCom în cadrul Serviciului European pentru Acțiuni Externe, pentru a monitoriza, analiza și răspunde campaniilor rusești de propagandă și dezinformare încadrate în spectrul amenințărilor hibride.

și dezintegrare a zonei euroatlantice. Unul dintre cele mai sensibile și vulnerabile domenii de dezinformare în funcționarea statelor membre ale UE se referă la procesele politice democratice, cum ar fi alegerile și referendumurile. Între noiembrie 2016 și aprilie 2019, ingerința Rusiei în procesele politice a afectat 16 din 20 de astfel de cazuri la nivel mondial (inclusiv în Marea Britanie, Franța, Germania și Spania) (Australian Strategic Policy Institute, 2020). Acestea au luat, în principal, forma unor campanii de dezinformare și atacuri cibernetice, inclusiv piratarea site-urilor web și modificarea conținutului acestora, atacuri asupra infrastructurii electorale sau furtul și publicarea de informații (hack and leak) pentru a manipula opinia publică.

În septembrie 2018, Uniunea a adoptat „Codul de practici", care guvernează cooperarea țărilor membre ale UE cu sectorul privat în ceea ce privește obligațiile pentru platformele online și industria de publicitate, cu scopul de a îmbunătăți transparența publicității politice, de a închide conturile false și de a reduce stimulentele pentru răspândirea dezinformarii.

Pentru a proteja alegătorii statelor membre ale UE de dezinformare și interferențe cibernetice, CERT-EU a creat un serviciu dedicat de *Social Media Assurance*, în vederea detectării și eliminării conturilor care uzurpă identitatea unui utilizator real. În septembrie 2018, Uniunea a adoptat, de asemenea, *„Codul de practici"*, care guvernează cooperarea țărilor membre ale UE cu sectorul privat în ceea ce privește obligațiile pentru platformele online și industria de publicitate, cu scopul de a îmbunătăți transparența publicității politice, de a închide conturile false și de a reduce stimulentele pentru răspândirea dezinformarii. Codul a fost adoptat, printre altele, de marile platforme de servicii online, precum Facebook, Google, Twitter și Microsoft. Aceștia s-au angajat să sporească transparența publicității politice și a finanțării acesteia și să îi blocheze pe cei responsabili de dezinformare. Aceste măsuri au avut ca scop protejarea alegerilor pentru Parlamentul European din mai 2019.

Busola strategică a anunțat crearea (până în 2023) a unui nou mecanism de creștere a conștientizării situației și a rezilienței UE, a statelor membre și a societăților acestora împotriva manipulării informațiilor și a interferenței în procesele politice (Foreign Information Manipulation and Interference Toolbox, FIMI). Noua platformă de colaborare își propune să standardizeze metodele de colectare, analiză și schimb de date (între guvernele statelor membre, sectorul privat și societatea civilă și organizațiile internaționale) cu privire la tacticile, tehnicile și procedurile utilizate de actorii care instrumentează amenințări hibride. Acest demers va spori capacitatea UE de a identifica și analiza din timp campaniile de dezinformare, va facilita colectarea

de dovezi ale interferențelor externe în procesele politice democratice și va standardiza metodele de raportare a unor astfel de incidente. Cel mai probabil, în scurt timp, va fi înființat un Centru de analiză și partajare a informațiilor (ISAC) ca parte a Setului de instrumente FIMI (StratCom activity report/Strategic Communication Task Forces and Information Analysis Division).

Consolidarea rezilienței țărilor membre ale UE se referă, de asemenea, la sectoare cheie precum securitatea cibernetică, infrastructura critică, energia, transporturile, apărarea, sistemul financiar, securitatea maritimă și spațiul (Kozioł, 2022). Acest efort este orientat, în primul rând, către construirea instrumentelor și capabilităților legale necesare pentru a răspunde incidentelor și crizelor cauzate de amenințările hibride (în special, în spațiul cibernetic). Un progres în abordarea UE cu privire la securitatea cibernetică a fost adoptarea, în 2016, a *„Directivei privind securitatea rețelelor și a sistemelor informatice"* (Directiva NIS). Aceasta obligă statele membre să garanteze standarde minime comune pentru securitatea cibernetică, inclusiv prin adoptarea unor norme naționale, strategii de securitate cibernetică sau crearea de echipe de răspuns la incidente informatice care operează în cadrul rețelei europene CERT. De asemenea, UE a stabilit ca raportarea incidentelor cibernetice să fie obligatorie pentru furnizorii de servicii cheie din sectoarele energiei, transporturilor, bancar și financiar, asistenței medicale, aprovizionării cu apă și infrastructurii digitale. Pe lângă activitățile de reglementare, UE, prin Agenția Europeană pentru Securitatea Rețelelor și a Informațiilor (ENISA) și Organizația Europeană pentru Securitate Cibernetică (ECSO), sprijină și activitățile de cercetare și cooperarea public-privat. Capabilitățile comune de apărare cibernetică ale statelor membre sunt, la rândul lor, dezvoltate prin intermediul a patru proiecte de cooperare structurată PESCO privind schimbul de informații referitoare la incidentele cibernetice, coordonarea activităților, sprijin și răspuns comun, precum și cercetare și formare (The Council of the European Union, 2019).

Consolidarea rezilienței țărilor membre ale UE se referă la sectoare cheie precum securitatea cibernetică, infrastructura critică, energia, transporturile, apărarea, sistemul financiar, securitatea maritimă și spațiul. Acest efort este orientat, în primul rând, către construirea instrumentelor și capabilităților legale necesare pentru a răspunde incidentelor și crizelor cauzate de amenințările hibride (în special, în spațiul cibernetic).

În decembrie 2020, Uniunea a adoptat o nouă strategie de securitate cibernetică, aceasta urmărind să sporească reziliența statelor membre la atacurile cibernetice și să le protejeze mai bine infrastructura critică (Comisia Europeană, 2020). Un exemplu de acțiune sectorială în acest

domeniu este setul de instrumente pentru diplomația cibernetică a UE, care conține măsuri ce acționează ca un factor de descurajare pentru potențialii atacatori cibernetici. Entitățile (aflate pe lista neagră) responsabile pentru atacuri cibernetice sau care susțin atacurile cibernetice împotriva statelor membre ale UE vor fi sancționate prin interdicția de a intra în UE și/sau prin înghețarea activelor lor. Un regim similar de sancțiuni a fost introdus împotriva țărilor care folosesc arme chimice (lista clasificată conține 20 de substanțe), ceea ce reprezintă răspunsul direct al UE la utilizarea agentului paralitic-convulsiv *„Novichok”* pe teritoriul Regatului Unit de către serviciile speciale ruse. Între 2019 și 2022, UE a oferit și sprijin financiar, în valoare de 11,6 milioane de euro, Organizației pentru Interzicerea Armelor Chimice (OPCW), pentru a contracara dezvoltarea și utilizarea armelor chimice.

Busola strategică a UE subliniază importanța consolidării capabilităților Uniunii de a răspunde unei crize generate de un atac de natură hibridă. Uniunea Europeană a anunțat crearea echipelor de răspuns rapid hibrid (EURHRT) până la sfârșitul anului 2024, pentru a sprijini statele membre în situații de atacuri hibride. De asemenea, este posibil ca aceste echipe să poată fi utilizate pentru misiunile și operațiile UE, precum și pentru a oferi asistență țărilor partenere.

PREVENIREA ȘI RĂSPUNSUL LA CRIZE

Busola strategică a UE subliniază importanța consolidării capabilităților Uniunii de a răspunde unei crize generate de un atac de natură hibridă. Uniunea Europeană a anunțat crearea echipelor de răspuns rapid hibrid (EURHRT) până la sfârșitul anului 2024, pentru a sprijini statele membre în situații de atacuri hibride. De asemenea, este posibil ca aceste echipe să poată fi utilizate pentru misiunile și operațiile UE, precum și pentru a oferi asistență țărilor partenere. Deși lucrările privind înființarea EURHRT-urilor se află în faza conceptuală, acestea vor fi, cel mai probabil, formate în conformitate cu echipele NATO de sprijin împotriva amenințărilor hibride (CHST) înființate în 2018. CHST-urile sunt instrumentul NATO de răspuns la amenințările hibride situate sub pragul de apărare colectivă prevăzut la articolul 5 din Tratatul Atlanticului de Nord. Până în prezent, CHST-urile au fost folosite de două ori: mai întâi în 2019, în Muntenegru, în legătură cu atacurile cibernetice și dezinformarea din perioada electorală, iar în 2021, în Lituania, în legătură cu criza migrației la graniță, susținută de Belarus. Echipele sunt compuse, în principal, din experți civili în domeniul strategic, comunicații, securitate cibernetică, contrainformații, securitate energetică și protecția infrastructurii critice. De asemenea, pot fi completate cu consilieri militari,

dacă situația impune o astfel de abordare. Într-o criză, aceștia pot fi dislocați într-un stat membru (la cererea acestuia) sau pot acționa ca o echipă de consiliere pentru a înființa structuri naționale de apărare pentru a contracara amenințările hibride (Rühle, Roberts, 2021).

IMPORTANȚA COOPERĂRII CU NATO

Busola strategică subliniază importanța cooperării în combaterea amenințărilor hibride cu parteneri precum G7, ONU și NATO. Uniunea atribuie un rol cheie în acest sens relațiilor sale cu Alianța Nord-Atlantică. În 2015, NATO a adoptat *„Strategia împotriva amenințărilor hibride”*, care are trei componente: pregătirea pentru atacuri hibride prin îmbunătățirea capabilităților de recunoaștere și avertizare timpurie, consolidarea protecției infrastructurii critice și testarea proceselor de luare a deciziilor în cadrul Alianței; descurajarea unui potențial agresor prin impunerea de sancțiuni și păstrarea incertitudinii cu privire la natura răspunsului, precum și apărarea aliaților în cazul unei agresiuni hibride.

În declarațiile comune din 2016 și 2018, UE și NATO au elaborat o listă de 74 de acțiuni comune în ceea ce privește dimensiunea de securitate, dintre care peste 20 pot fi legate de combaterea amenințărilor hibride. Accentul se pune, în primul rând, pe recunoașterea fenomenului, creșterea conștientizării situației, construirea rezilienței societale, protejarea infrastructurii critice și răspunsul la urgențele generate de amenințările hibride. Ambele organizații lucrează pentru a implementa inițiative comune bazate pe mecanisme sistemice de cooperare între personalul propriu, pe trei niveluri interdependente: expert, intermediar (în cadrul grupului central UE-NATO) și strategic (Grupul de conducere UE-NATO). Prin cooperare informală, organizațiile au dezvoltat un protocol operațional comun pentru împărtășirea cunoștințelor privind operațiile hibride și coordonarea răspunsurilor ambelor instituții. Cadrul comun a stabilit ambiția fără echivoc de a face din combaterea amenințărilor hibride o prioritate a UE.

În 2015, NATO a adoptat „Strategia împotriva amenințărilor hibride”, care are trei componente: pregătirea pentru atacuri hibride prin îmbunătățirea capabilităților de recunoaștere și avertizare timpurie, consolidarea protecției infrastructurii critice și testarea proceselor de luare a deciziilor în cadrul Alianței; descurajarea unui potențial agresor prin impunerea de sancțiuni și păstrarea incertitudinii cu privire la natura răspunsului, precum și apărarea aliaților în cazul unei agresiuni hibride.

Prima inițiativă comună UE-NATO privind combaterea amenințărilor hibride a fost înființarea Centrului European de Excelență (Hybrid CoE) la Helsinki (2016). Acesta acționează ca un think-tank, ce oferă expertiză și asistență consultativă și o platformă pentru schimbul

de experiență și informații cu privire la amenințările hibride. Centrul de la Helsinki contribuie, în primul rând, la cunoașterea situației pentru ambele organizații, la fel ca Celula de fuziune hibridă a UE sau omologul său, Filiala de analiză hibridă a NATO, care operează în cadrul Diviziei comune de informații și securitate (JISD). Ambele structuri au relații de lucru bine stabilite prin schimburi lunare de personal. Celulele de analiză a amenințărilor hibride UE și NATO pregătesc, de asemenea, evaluări comune ale amenințărilor (evaluări paralele și coordonate). O cooperare similară este, de asemenea, dezvoltată între Grupul de lucru East StratCom și Centrul de excelență al NATO pentru comunicații strategice (StratCom CoE) din Riga, elaborând materiale de instruire comune, cursuri de răspuns la dezinformare și alte instrumente pentru personalul UE și al NATO.

Din 2017, UE și NATO desfășoară exercițiul EU Integrated Resolve și Exercițiul NATO de gestionare a crizelor (CMX) în formatul exerciții paralele și coordonate (PACE) pentru a testa capacitatea de a răspunde la crize (inclusiv evenimente hibride) printr-un protocol operațional comun. În fiecare an, exercițiul schimbă organizația principală: în 2022 – UE, în 2023 – NATO.

La nivel practic, Hybrid CoE este responsabil cu organizarea de ateliere, seminarii și exerciții, care includ simulări ale reuniunilor Consiliului Atlanticului de Nord (NAC) și ale Comitetului Politic și de Securitate (PSC) în timpul atacurilor hibride. Din 2017, UE și NATO desfășoară exercițiul EU *Integrated Resolve* și Exercițiul NATO *de gestionare a crizelor* (CMX) în formatul exerciții paralele și coordonate (PACE) pentru a testa capacitatea de a răspunde la crize (inclusiv evenimente hibride) printr-un protocol operațional comun. În fiecare an, exercițiul schimbă organizația principală: în 2022 – UE, în 2023 – NATO. Organizațiile caută, de asemenea, oportunități pentru răspunsuri comune (complementare) la amenințările din spațiul cibernetic, facilitate de antrenamente și exerciții comune (de exemplu, *Cyber Phalanx*, *Locked Shields* sau Coaliția cibernetică NATO), schimb de informații și documente doctrinare, contacte regulate de lucru, educație, proiecte și altele. Această cooperare are loc prin intermediul Agenției Europene de Apărare (EDA) și al Centrului de excelență al NATO pentru apărare cibernetică din Tallinn, printre altele. Un element important al acesteia este cooperarea în dimensiunea tehnologică, inclusiv schimbul de experiență și practici între CERT-EU și NATO Computer Incident Response Capability (NCIRC) la Comandamentul Suprem al Forțelor Aliate din Europa (SHAPE).

CONCLUZII

Crearea setului de instrumente al UE pentru răspunsul la amenințările hibride va consolida capacitatea Uniunii de a contracara și de a răspunde acestor tipuri de amenințări. Setul cuprinzător de măsuri, care a fost în curs de dezvoltare din 2016, se caracterizează prin flexibilitate de răspuns și deschidere către identificarea noilor metode și tactici hibride utilizate atât de actorii statali, cât și de cei non-statali. Sarcina de a răspunde la acțiuni hibride ostile revine statelor membre [în conformitate cu articolul 4 alineatul (2) TUE], în timp ce rolul Uniunii este de a le sprijini și de a coordona răspunsurile comune la crize. Implementarea de noi instrumente și *modus operandi* va crește, printre altele, conștientizarea situației și reziliența instituțiilor UE, a statelor membre și a societăților acestora (în special, împotriva manipulării informațiilor și a interferenței străine în procesele democratice).

Crearea setului de instrumente al UE pentru răspunsul la amenințările hibride va consolida capacitatea Uniunii de a contracara și de a răspunde acestor tipuri de amenințări. Setul cuprinzător de măsuri, care a fost în curs de dezvoltare din 2016, se caracterizează prin flexibilitate de răspuns și deschidere către identificarea noilor metode și tactici hibride utilizate atât de actorii statali, cât și de cei non-statali.

Datorită cooperării multilaterale în domeniul informațiilor, înființării celulei hibride de fuziune și a sistemului de avertizare timpurie a dezinformarii, Uniunea Europeană și-a îmbunătățit în mod semnificativ cunoașterea situației. Complexitatea amenințărilor hibride și extinderea anticipată a sectoarelor de interes strategic (inclusiv securitatea sănătății, schimbările climatice, protecția mediului sau noile tehnologii) generează nevoia de a consolida capabilitățile analitice ale acestor structuri prin creșterea personalului și a resurselor financiare. Este în interesul României, ca stat membru al UE și al NATO, să aibă reprezentanți (diplomați, specialiști, militari, experți de domeniu) în aceste structuri (în special, în funcții de conducere). Acest lucru va face posibilă elaborarea sincronizată și implementarea într-o mai mare măsură a documentelor programatice și doctrinare în domeniul amenințărilor hibride.

Crearea planificată de noi instrumente pentru identificarea campaniilor de dezinformare și a interferențelor în procesele politice (FIMI) sau de răspuns la crize hibride (EURHRT) este doar la stadiul conceptual. Cu toate acestea, *Busola strategică* a UE nu precizează din ce elemente vor fi compuse și în ce condiții pot fi utilizate. De aceea, România ar trebui să aibă în vedere ca EURHTR-urile UE să fie pregătite să sprijine statele membre, misiunile și operațiile UE și să consolideze reziliența statelor partenere expuse la acțiuni hibride ostile, cum sunt Republica Moldova, Georgia și altele.

BIBLIOGRAFIE:

1. Dyner, A.M. (2002). *„The Border Crisis as an Example of Hybrid Warfare”*. În *PISM Strategic File*, nr. 2, februarie, https://www.pism.pl/publications/the-border-crisis-as-an-example-of-hybrid-warfare, accesat la 24 august 2022.
2. Kaca, *E. (2021). „Sancțiunile UE pentru campaniile de dezinformare: perspective și limite”*. În *Buletinul PISM*, nr. 104, 26 mai 2021, www.pism.pl., accesat la 25 august 2022.
3. Kozioł, A. (2022). *„Strategic Compass: Towards EU Space Strategy for Security and Defense”*. În *Policy Paper PISM*, nr. 1, https://www.pism.pl/publications/strategic-compass-towards-eu-space-strategy-for-security-and-defence, accesat la 1 septembrie 2022.
4. O’Connor, S., Hanson, F., Currey, E., Beattie, T. (2020). *„Cyber-enabled foreign interference in elections and referendums”*. Australian Strategic Policy Institute, 28 octombrie 2020, https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums, accesat la 1 septembrie 2022.
5. Rühle, M., Roberts, C. (2021). *„Enlarging NATO’s toolbox to counter hybrid threats”*, 19 martie 2021, https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html, accesat la 2 septembrie 2022.
6. Ștefan, M. (2020). *„Intelligence versus fake news în contextul COVID 19”.* În revista *INFOSFERA*, nr. 2, ISSN 2065-3395, pp. 35-43.
7. *„Cadrul comun pentru combaterea amenințărilor hibride, un răspuns al Uniunii Europene”* (2016). Comisia Europeană, 6 aprilie 2016, https://eur-lex.europa.eu., accesat la 8 august 2022.
8. *„Complementary efforts to enhance resilience and counter hybrid threats – Council Conclusions”* (2019). The Council of the European Union, 10 decembrie 2019, https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf., accesat la 5 iulie 2022.
9. *„Concluziile Consiliului European din 21 și 22 octombrie 2021”*. Consiliul Europei, https://www.consilium.europa.eu/media/52622/20211022-euco-conclusions-en.pdf., accesat la 17 august 2022.
10. *„Rezoluție privind clauza de apărare reciprocă (articolul 42 alineatul (7) TUE)”*. Parlamentul European, https://oeil.secure.europarl.europa.eu., accesat la 26 august 2022.
11. *„Strategia UE de securitate cibernetică pentru deceniul digital”* (2020). Comisia Europeană, 16 decembrie 2020, https://digital-strategy.ec.europa.eu., accesat la 12 mai 2022.
12. *„2021 StratCom activity report – Strategic Communication Task Forces and Information Analysis Division”* (24 martie 2022), https://www.eeas.europa.eu., accesat la 27.04.2022.
13. https://euvsdisinfo.eu/ro/#, accesat la 11 august 2022.
14. https://www.consilium.europa.eu/ro/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/, accesat la 29 august 2022.
15. https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11232, accesat la 28 august 2022.
16. https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf., accesat la 28 august 2022.
17. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf, accesat la 29 august 2022.
18. https://www.nato.int/cps/en/natohq/topics_156338.htm., accesat la 22 august 2022.