



ÎNALTUL REPREZENTANT AL
UNIUNII PENTRU AFACERI
EXTERNE ȘI POLITICA
DE SĂCURITATE

Bruxelles, 19.7.2017
JOIN(2017) 30 final

RAPORT COMUN CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

**referitor la punerea în aplicare a Cadrului comun privind contracararea amenințărilor
hibride - Un răspuns al Uniunii Europene**

1. INTRODUCERE

UE se confruntă cu una dintre cele mai mari provocări din istoria sa în domeniul securității. Amenințările îmbracă forme din ce în ce mai neconvenționale, unele dintre acestea fiind fizice, precum noile forme de terorism, iar altele utilizând spațiul digital pentru lansarea unor atacuri cibernetice complexe. Alte tipuri de amenințări sunt mai subtile și urmăresc aplicarea coercitivă a presiunii, incluzând campaniile de dezinformare și manipularea prin mass-media. Scopul lor este subminarea valorilor europene, precum demnitatea umană, libertatea și democrația. Recentele atacuri cibernetice coordonate la nivel mondial, a căror origine s-a dovedit a fi greu de identificat, au pus în evidență punctele vulnerabile ale societăților și instituțiilor noastre.

În aprilie 2016, Comisia Europeană și Înalțul Reprezentant au adoptat o Comunicare comună privind contracararea amenințărilor hibride¹ (Cadrul comun). Recunoscând natura complexă și transfrontalieră a amenințărilor hibride, acest cadru propune o abordare la nivelul întregii administrații pentru a consolida reziliența în ansamblu a societăților noastre. Consiliul² a salutat inițiativa și acțiunile propuse, invitând în același timp Comisia și Înalțul reprezentant să prezinte, în iulie 2017, un raport privind progreselor înregistrate. În vreme ce UE poate sprijini statele membre să-și consolideze reziliența împotriva amenințărilor hibride, responsabilitatea principală le revine statelor membre, întrucât contracararea amenințărilor hibride intră în domeniul politicilor naționale de securitate și apărare.

Acest cadru comun pentru contracararea amenințărilor hibride constituie o parte importantă a politicii globale a UE de abordare mai integrată a securității și apărării. El contribuie la crearea unei Europe care protejează, așa cum a solicitat președintele Juncker în discursul privind starea Uniunii din septembrie 2016. În 2016, Uniunea Europeană a pus bazele unei politici europene de apărare consolidate pentru a răspunde așteptărilor cetățenilor de a dispune de mai multă protecție. Strategia globală a UE pentru politica externă și de securitate a UE³ a subliniat necesitatea unei abordări integrate pentru a face legătura între reziliența internă și acțiunile externe ale UE și a făcut apel la crearea unei sinergii între politica de apărare și politicile privind piața internă, industria, asigurarea aplicării legii și serviciile de informații. În urma adoptării, în noiembrie 2016, a planului de acțiune european în domeniul apărării, Comisia a prezentat o serie de inițiative concrete care vor contribui la consolidarea capacității UE de a răspunde amenințărilor hibride, prin promovarea rezilienței în lanțurile de aprovizionare pentru apărare și prin consolidarea pieței unice a apărării. În special, la 7 iunie 2017, Comisia a lansat Fondul european de apărare, cu o finanțare propusă de 600 de milioane EUR până în 2020 și de 1,5 miliarde EUR pe an după 2020. Comunicarea privind uniunea securității⁴ a recunoscut necesitatea de a contracara amenințările hibride și faptul că este important să se asigure o mai mare coerență între acțiunile interne și cele externe în materie de securitate.

¹ Comunicare comună către Parlamentul European și Consiliu *Cadrul comun privind contracararea amenințărilor hibride - Un răspuns al Uniunii Europene*, JOIN (2016) 18 final.

² *Concluzii ale Consiliului privind combaterea amenințărilor hibride*, Comunicat de presă 196/16, 19 aprilie 2016.

³ A fost prezentată de Înalțul Reprezentant în cadrul Consiliului European la 28 iunie 2016.

⁴ COM(2016) 230 final, 20.4.2016.

Liderii UE au acordat securității și apărării un loc central în dezbaterile cu privire la viitorul Europei⁵. Acest lucru a fost recunoscut în **Declarația de la Roma** din 25 martie 2017, prin care se stabilește o viziune a unui climat de siguranță și securitate într-o Uniune hotărâtă să își consolideze politica de securitate și apărare. Președintele Consiliului European, președintele Comisiei Europene și Secretarul General al NATO au semnat o declarație comună la Varșovia, la 8 iulie 2016, cu scopul de a oferi un nou impuls și o nouă substanță parteneriatului strategic UE-NATO. Declarația comună a evidențiat șapte domenii concrete, inclusiv contracararea amenințărilor hibride, în care cooperarea dintre cele două organizații ar trebui să fie consolidată. Ulterior, Consiliul UE și Consiliul NATO au aprobat un set comun de 42 de propuneri pentru punerea în aplicare, iar în iunie 2017 a fost emis un prim raport, care indică progrese substanțiale⁶.

Cartea albă a Comisiei privind viitorul apărării europene⁷, publicată în iunie 2017, prezintă diferite scenarii cu privire la modul de abordare a amenințărilor din ce în ce mai mari la adresa securității și apărării cu care se confruntă Europa, precum și cu privire la modul de consolidare a capacităților de apărare ale Europei până în 2025. În toate cele trei scenarii, securitatea și apărarea sunt considerate parte integrantă a proiectului european, în vederea protejării și promovării intereselor noastre în Uniune și în străinătate. Europa trebuie să devină un furnizor de securitate și să își asigure în mod treptat propria securitate. Niciun stat membru nu poate face față provocărilor viitoare pe cont propriu, în special în ceea ce privește contracararea amenințărilor hibride. Cooperarea în domeniul apărării și securității nu este, prin urmare, o opțiune; ea este o necesitate pentru a construi o Europă care protejează.

Scopul prezentului raport este de a oferi o prezentare a următoarelor etape de punere în aplicare și a progreselor înregistrate în privința acțiunilor din cele patru domenii propuse în Cadrul comun: ameliorarea cunoașterii situației; consolidarea rezilienței; consolidarea capacității statelor membre și a Uniunii de a preveni crizele, de a reacționa la acestea și de a se redresa în mod coordonat și îmbunătățirea cooperării cu NATO pentru a asigura complementaritatea măsurilor. Raportul ar trebui citit împreună cu rapoartele lunare privind progresele către o uniune a securității efective și reale.

2. RECUNOAȘTEREA NATURII HIBRIDE A UNEI AMENINȚĂRI

Activitățile hibride devin o caracteristică frecventă a mediului de securitate european. Intensitatea acestor activități este în creștere, existând motive de îngrijorare tot mai mari legate de influențarea alegerilor, campaniile de dezinformare, activitățile cibernetice ostile și autorii de acte hibride care încearcă să îi radicalizeze pe membrii vulnerabili ai societății pentru a acționa apoi prin intermediul lor. Vulnerabilitățile constatate în raport cu amenințările hibride nu se limitează la frontierele naționale. Pentru a contracara amenințările hibride, este necesară coordonarea răspunsului și la nivelurile UE și NATO. Evoluțiile înregistrate începând din aprilie 2016 arată că, deși amenințările sunt adesea evaluate în mod izolat, există o recunoaștere și o înțelegere tot mai ample, în cadrul Uniunii, a naturii hibride a

⁵ Foaia de parcurs de la Bratislava a Consiliului European din 16 septembrie 2016 și Declarația de la Roma a șefilor de stat și de guvern din 27 de state membre și a Consiliului European, Parlamentului European și Comisiei Europene din 25 martie 2017.

⁶ <http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation>

⁷ Document de reflecție privind viitorul sistemului de apărare european, 7.6.2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf

unora dintre activitățile observate și a necesității unei acțiuni coordonate. UE își va continua eforturile de a îmbunătăți gradul de cunoaștere a situației și cooperarea.

Acțiunea 1: Statele membre, sprijinite, după caz, de Comisie și de Înaltul Reprezentant, sunt invitate să lanseze un studiu privind riscurile hibride pentru identificarea principalelor vulnerabilități, inclusiv indicatorii specifici de amenințări hibride, care pot afecta structurile și rețelele naționale și paneuropene.

Consiliul a înființat grupul „Prietenii Președinției”, care reunește experți din statele membre pentru a crea un sondaj generic care le-ar permite să identifice într-o măsură mai bună principalii indicatori ai amenințărilor hibride, să îi includă în mecanismele de alertă timpurie și în mecanismele existente de evaluare a riscurilor și să îi disemineze, dacă este cazul. Termenii de referință au fost conveniți, iar activitatea grupului a fost deja lansată. Sondajul generic ar trebui să fie gata înainte de sfârșitul anului 2017, sondajele propriu-zise urmând să înceapă după această dată. Protecția împotriva amenințărilor hibride ar trebui să se autoconsolideze. Prin urmare, statele membre sunt încurajate să efectueze aceste sondaje în cel mai scurt timp posibil, întrucât acestea vor furniza informații valoroase cu privire la gradul de vulnerabilitate și de pregătire din Europa.

a. ÎMBUNĂTĂȚIREA GRADULUI DE CUNOAȘTERE

Schimbul de analize ale informațiilor și de activități de evaluare este un instrument esențial pentru reducerea incertitudinii și îmbunătățirea gradului de cunoaștere a situației. În ultimul an s-au înregistrat progrese semnificative. A fost instituită celula de fuziune a UE împotriva amenințărilor hibride, care este în prezent pe deplin operațională, a fost constituit grupul operativ East StratCom, iar Finlanda a lansat Centrul european pentru contracararea amenințărilor hibride. Cea mai mare parte a activităților s-a axat pe analizarea instrumentelor și pârgھیilor de propagandă sau dezinformare, existând o bună cooperare în acest sens între grupul operativ East StratCom, celula de fuziune a UE împotriva amenințărilor hibride și NATO. Aceasta constituie o bază solidă pentru a continua consolidarea unei culturi mai aprofundate de analiză și evaluare a amenințărilor la adresa securității noastre interne și externe prin intermediul unei abordări adaptate la amenințările hibride.

Celula de fuziune împotriva amenințărilor hibride

Acțiunea 2: Crearea unei celule de fuziune a UE împotriva amenințărilor hibride în cadrul structurii existente a Centrului de analiză a informațiilor al UE, care să fie în măsură să primească și să analizeze informațiile clasificate și pe cele din surse deschise privind amenințările hibride. Statele membre sunt invitate să creeze puncte de contact naționale privind amenințările hibride pentru a asigura cooperarea și comunicarea securizată cu celula de fuziune a UE împotriva amenințărilor hibride.

Celula de fuziune a UE împotriva amenințărilor a fost instituită în cadrul Centrului de analiză a informațiilor al UE pentru a primi și analiza informații clasificate și informații din surse deschise provenind de la diferite părți interesate referitoare la amenințările hibride. Analiza este apoi distribuită în cadrul UE și în rândul statelor membre și furnizează informații pentru procesele decizionale de la nivelul UE, inclusiv contribuții pentru studiile de evaluare a riscurilor privind securitatea realizate la nivelul UE. Divizia de informații a Statului-Major al UE contribuie la activitatea celulei de fuziune cu analize militare. Până în prezent, au fost realizate peste 50 de evaluări și informări privind subiecte legate de acțiunile hibride. Începând cu luna ianuarie 2017, celula a lansat „Hybrid bulletin”, o publicație periodică de

analiză a amenințărilor actuale și a chestiunilor hibride, distribuită în mod direct în cadrul instituțiilor și al organismelor UE și la punctele naționale de contact⁸. Capacitatea operațională deplină a celulei a fost atinsă în mai 2017, conform planificării. În fine, angajamentul direct, la nivel de personal, cu noua filială de analize hibride a NATO este în curs de desfășurare, atât în ceea ce privește împărtășirea experienței acumulate la crearea celulei de fuziune, cât și în ceea ce privește schimbul de informații (efectuat cu respectarea deplină a normelor UE cu privire la schimbul de informații clasificate). Celula de fuziune a UE împotriva amenințărilor hibride a început identificarea unor noi inițiative pentru a impulsiona cooperarea pe viitor și va juca un rol esențial în exercițiile paralele UE-NATO planificate pentru toamna anului 2017, în cadrul cărora va fi testată capacitatea de răspuns a celulei de fuziune a UE împotriva amenințărilor hibride, urmând ca învățămintele trase să fie asimilate.

Comunicarea strategică

Acțiunea 3: Înaltul Reprezentant va examina împreună cu statele membre modalitățile de actualizare și coordonare a capacităților de realizare a unei comunicări strategice proactive și de optimizare a utilizării serviciilor oferite de specialiști în domeniul monitorizării mass-mediei și în domeniul lingvistic.

În ultimele luni, din seria de mijloace utilizate pentru a submina adversarii au făcut parte campaniile de dezinformare din ce în ce mai ample și răspândirea de știri false prin rețelele sociale. În cazurile în care platformele preferate sunt rețelele sociale, informații care în aparență sunt fiabile și legitime pot schimba opinia publică în beneficiul unor persoane fizice, organizații sau guverne. Aceste tactici hibride au un obiectiv mai amplu, și anume de a genera confuzie în societățile noastre și a discredita guvernele democratice și structurile, instituțiile și alegerile noastre. Deseori, știrile false sunt difuzate prin intermediul platformelor online (a se vedea, de asemenea, acțiunea 17). Comisia și Înaltul Reprezentant salută măsurile recente luate de platformele online și de editorii de presă pentru a combate dezinformarea. Comisia va continua să încurajeze astfel de măsuri voluntare.

Înaltul Reprezentant a instituit grupul operativ East Stratcom, care anticipează cazurile și campaniile de dezinformare și le combate. Această măsură îmbunătățește radical comunicarea privind politicile Uniunii în vecinătatea estică, consolidând în același timp peisajul mass-media din aceste țări. În ultimii doi ani, grupul operativ a identificat peste 3 000 de cazuri separate de dezinformare în 18 limbi. Viitoarea lansare a unui nou site web: „#EUvsdisinformation”, care include un motor de căutare online, va îmbunătăți în mod semnificativ accesul la informații reale al utilizatorilor. Cu toate acestea, cercetările și activitatea analitică arată că numărul de canale și de mesaje de dezinformare difuzate zilnic este mult mai ridicat. Proiectul EU-STRAT, finanțat prin programul Horizon 2020, analizează politicile și mass-media din țările din cadrul Parteneriatului estic.

Înaltul Reprezentant invită statele membre să sprijine activitatea grupurilor operative StratCom pentru a contracara mai eficient tendința de creștere a amenințărilor hibride. Acest lucru va ajuta grupul operativ South să îmbunătățească comunicarea și contactele cu statele arabe, inclusiv în limba arabă, să combată ideile preconcepute și să prezinte factual Uniunea Europeană și politicile sale. Interacțiunea cu jurnaliștii de la nivel local va contribui la

⁸ Până în prezent, 21 de state membre au desemnat puncte de contact naționale. Acestea sunt persoane care lucrează în capitale ale statelor membre, ocupând un post cu profil din domeniul politicilor/al rezilienței.

asigurarea sincronizării știrilor din punct de vedere cultural. Ambele grupuri operative, asistate de celula de fuziune a UE împotriva amenințărilor hibride, au obiectivul de a sprijini și suplimenta eforturile în acest domeniu ale statelor membre. În plus, Comisia cofinanțează Rețeaua de comunicații strategice europene, o rețea de colaborare a 26 de state membre care împărtășește analize, bune practici și idei privind utilizarea comunicațiilor strategice la combaterea extremismului violent, inclusiv privind dezinformarea.

Centrul de excelență pentru „contracurarea amenințărilor hibride”

Acțiunea 4: Statele membre sunt invitate să înființeze un Centru de excelență pentru „contracurarea amenințărilor hibride”.

Ca răspuns la apelul de a înființa un centru de excelență, în aprilie 2017, Finlanda a lansat Centrul european pentru contracurarea amenințărilor hibride. Zece state membre ale UE⁹, Norvegia și SUA sunt membre fondatoare, în timp ce Uniunea Europeană și NATO au fost invitate să sprijine Comitetul director¹⁰. Misiunea centrului este de a încuraja dialogul strategic, precum și de a desfășura activități de cercetare și analiză, de a coopera cu comunitățile de interese pentru a îmbunătăți reziliența și capacitatea de reacție, toate acestea în scopul de a contribui la contracurarea amenințărilor hibride. Centrul ar trebui să funcționeze, de asemenea, ca o platformă pentru viitoarele exerciții hibride. Centrul a stabilit deja legături strânse cu celula de fuziune a UE împotriva amenințărilor hibride, iar activitățile desfășurate de cele două organizații ar trebui să se completeze reciproc. UE analizează în prezent modalitățile prin care poate oferi un sprijin concret Centrului.

b. CONSOLIDAREA REZILIENȚEI

Cadrul comun plasează reziliența (de exemplu, a transportului, comunicațiilor, energiei, finanțelor sau a infrastructurilor regionale de securitate) în centrul acțiunilor UE de combatere a campaniilor de propagandă și de dezinformare, a tentativelor de subminare a activităților întreprinderilor, a fluxurilor sociale și economice, precum și a atacurilor asupra infrastructurilor cibernetice și asupra tehnologiei informației. Cadrul consideră consolidarea rezilienței drept o acțiune preventivă și de descurajare, al cărei obiectiv este de a consolida societățile și a evita escaladarea crizelor, atât în interiorul, cât și în afara UE. Valoarea adăugată a UE constă în sprijinul acordat statelor membre și partenerilor pentru a-și dezvolta reziliența, apelând la o gamă largă de instrumente și programe existente. Au fost înregistrate progrese semnificative în privința acțiunilor de consolidare a rezilienței în domenii precum securitatea cibernetică, infrastructura critică, protejarea sistemului financiar de utilizările ilicite, precum și în ceea ce privește eforturile de combatere a extremismului violent și a radicalizării.

Protejarea infrastructurilor critice

Acțiunea 5: Comisia, în cooperare cu statele membre și cu părțile interesate, va identifica instrumente comune, inclusiv indicatori, în vederea îmbunătățirii protecției și rezilienței infrastructurilor critice împotriva amenințărilor hibride în sectoarele relevante.

⁹ Finlanda, Franța, Germania, Letonia, Lituania, Polonia, Suedia, Regatul Unit, Estonia, Spania.

¹⁰ Centrul oferă celorlalte state membre ale UE și altor membri NATO posibilitatea de a participa la aceasta inițiativă în calitate de membri.

În contextul Programului european privind protecția infrastructurilor critice (PEPIC), Comisia a continuat să depună eforturi pentru a identifica instrumente comune, inclusiv indicatori de vulnerabilitate, pentru îmbunătățirea rezilienței infrastructurilor critice împotriva amenințărilor hibride în sectoarele relevante. În mai 2017, Comisia a organizat un atelier de lucru privind amenințările hibride la adresa infrastructurilor critice, la care au participat reprezentanți din aproape toate statele membre, operatori din sectorul infrastructurilor critice, celula de fuziune a UE împotriva amenințărilor hibride, precum și NATO în calitate de observator. Au fost convenite o foaie de parcurs și măsuri pentru activitățile viitoare, pe baza unui chestionar transmis autorităților naționale din statele membre. Comisia va continua să consulte părțile interesate în toamna acestui an, cu scopul de a ajunge la un acord cu privire la indicatori până la sfârșitul anului 2017.

Agenția Europeană de Apărare (AEA) depune eforturi pentru a identifica deficiențele capacităților comune și ale sectorului comun al cercetării cauzate de legătura existentă între infrastructurile energetice și capacitățile de apărare. Agenția Europeană de Apărare va elabora un document conceptual în toamna anului 2017, precum și acțiuni-pilot destinate metodologiilor globale.

Cresterea securității aprovizionării cu energie a UE

Acțiunea 6: Comisia, în cooperare cu statele membre, va sprijini eforturile de diversificare a surselor de energie și de promovare a standardelor de securitate și de siguranță în vederea sporirii rezilienței infrastructurilor nucleare.

În decembrie 2016, Comisia a făcut propuneri concrete în pachetul privind securitatea aprovizionării, iar în aprilie 2017, Consiliul și Parlamentul European au ajuns la un acord cu privire la noul regulament privind securitatea aprovizionării cu gaz, al cărui scop este să prevină crizele de aprovizionare cu gaze. Noile norme vor garanta o coordonare la nivel regional și abordări comune ale statelor membre în ceea ce privește măsurile legate de securitatea aprovizionării. Aceste norme vor îmbunătăți capacitatea Uniunii Europene de a se pregăti pentru o eventuală penurie de gaze naturale și de a gestiona o astfel de situație, în cazul unei crize sau al unui atac hibrid. Pentru prima dată, se va aplica principiul solidarității: statele membre vor fi în măsură să își ajute vecinii în caz de criză gravă sau de atac, astfel încât gospodăriile și întreprinderile europene să nu se confrunte cu întreruperi ale furnizărilor cu gaze.

De asemenea, UE a înregistrat progrese în ceea ce privește elaborarea de proiecte-cheie care vizează diversificarea rutelor și surselor sale de aprovizionare cu energie, în conformitate cu strategia-cadru pentru o uniune energetică și cu Strategia europeană pentru securitate energetică. De exemplu, pe coridorul sudic al gazelor, sunt în curs de desfășurare lucrări de construcții la toate marile proiecte de gazoducte: extinderea gazoductului din Caucazul de Sud, a gazoductelor transanatolian și transadriatic, a exploatării Shah Deniz II în amonte, precum și extinderea coridorului sudic al gazelor către Asia Centrală, în special către Turkmenistan. Importurile de gaz natural lichefiat (GNL) în Europa sunt în continuă creștere și provin din surse noi, cum ar fi Statele Unite ale Americii. Exemplul terminalului din Lituania demonstrează modul în care proiectele de diversificare pot reduce dependența de un singur furnizor. Depunerea unor eforturi suplimentare în sectorul energetic și o mai bună utilizare a surselor de energie locale, în special a celor regenerabile, contribuie de asemenea la diversificarea rutelor și a surselor de energie.

În domeniul securității nucleare, Comisia sprijină în mod activ, în special prin ateliere de lucru organizate împreună cu autoritățile naționale și cu organismele de reglementare, o punere în aplicare coerentă și eficace a celor două directive privind securitatea nucleară și standardele de siguranță de bază, pe care statele membre trebuie să le transpună până la sfârșitul anului 2017, respectiv 2018. De asemenea, programul Euratom pentru cercetare și formare contribuie la sporirea securității nucleare.

Securitatea transporturilor și a lanțurilor de aprovizionare

Acțiunea 7: Comisia va monitoriza amenințările emergente în ansamblul sectorului transporturilor și va actualiza legislația, acolo unde este cazul. În cadrul punerii în aplicare a Strategiei UE în materie de securitate maritimă, precum și a strategiei și a planurilor lor de acțiune pentru gestionarea riscurilor vamale ale UE, Comisia și Înalțul Reprezentant (în limitele competențelor lor respective), în coordonare cu statele membre, vor examina modalitățile de a răspunde la amenințările hibride, în special la cele referitoare la infrastructurile de transport critice.

Conform comunicării privind uniunea securității, Comisia facilitează evaluările riscurilor în materie de securitate la nivelul UE cu statele membre, cu Centrul de analiză a informațiilor al UE și cu agențiile relevante pentru a identifica amenințările la adresa securității transportului și a sprijini elaborarea unor măsuri de atenuare eficace și proporționale. Doborârea, în 2014, în estul Ucrainei, a aeronavei care efectua zborul MH17 al companiei Malaysia Airlines a scos în evidență riscul reprezentat de survolarea zonelor de conflict. În conformitate cu recomandările grupului operativ european la nivel înalt privind zonele de conflict¹¹, Comisia a elaborat o metodologie pentru „evaluarea comună a riscurilor, efectuată la nivelul UE” cu sprijinul experților de la nivel național din sectoarele aeronautic și al securității și cu sprijinul SEAE, care să permită schimbul de informații clasificate și definirea unei viziuni comune a riscurilor. În martie 2017, Agenția Europeană de Siguranță a Aviației (EASA) a publicat primul „Conflict Zones Information Bulletin (Buletin de informare privind zonele de conflict)”¹² pe baza rezultatelor acestei evaluări comune a riscurilor, efectuate la nivelul UE. Comisia ia în calcul extinderea la alte moduri de transport (de exemplu, feroviar, maritim) a activităților de evaluare a riscurilor desfășurate în sectorul aeronautic, iar propunerile vor fi prezentate în 2018. În iunie 2017, Comisia, SEAE și statele membre au lansat un exercițiu de evaluare a riscurilor privind securitatea feroviară pentru a identifica carențele și măsurile posibile pentru atenuarea riscurilor.

De asemenea, în cadrul proiectelor de cercetare din domeniul securității finanțate prin cel de-al șaptelea program-cadru și prin programul Orizont 2020, a fost acordată o atenție specială domeniilor securității aeronautice și al managementului traficului aerian (ATM). În sectorul aviației civile, Comisia, împreună cu Agenția Europeană de Siguranță a Aviației și cu părțile interesate, pregătește în prezent două noi inițiative pentru îmbunătățirea securității cibernetice, care sunt destinate inclusiv contracarării amenințărilor hibride: înființarea unei centru de răspuns la incidente de securitate cibernetică din sectorul aeronautic și instituirea unui grup operativ privind securitatea cibernetică în cadrul Întreprinderii comune de cercetare în domeniul managementului traficului aerian din cadrul cerului unic european (SESAR), responsabilă cu managementul traficului aerian în cadrul cerului unic european. Agenția Europeană de Apărare furnizează informații militare cu privire la securitatea cibernetică în

¹¹https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

¹²<https://ad.easa.europa.eu/czib-docs/page-1>

sectorul aeronautic, atât Întreprinderii comune SESAR, cât și Agenției Europene de Siguranță a Aviației, prin intermediul platformei de cooperare strategică europeană privind securitatea cibernetică. La cererea statelor membre și a industriei de profil, această platformă va sprijini coordonarea la nivelul UE a tuturor activităților din sectorul aeronautic. În conformitate cu foaia de parcurs privind securitatea cibernetică în domeniul aviației, Agenția Europeană de Siguranță a Aviației a efectuat, în 2016, analize pentru determinarea curențelor actualelor norme și, în special, pentru definirea și instituirea Centrului european pentru securitatea cibernetică în sectorul aeronautic; acest centru este în prezent operațional și cooperează cu centrul de răspuns la incidente de securitate cibernetică din sectorul aeronautic al UE (CERT-UE) (memorandul de înțelegere a fost semnat în februarie 2017), furnizând analize ale amenințărilor din sectorul aeronautic, precum și cu EUROCONTROL (fiind deja adoptată o foaie de parcurs pentru cooperare); pe de altă parte, a fost lansat un site web pentru publicarea analizelor provenite din surse deschise. Până în toamna anului 2017, vor fi adoptate un program de standardizare și un protocol pentru schimbul securizat de informații.

Gestionarea riscurilor vamale

În ceea ce privește sectorul vămilor, Comisia se concentrează pe îmbunătățirea semnificativă a informațiilor prelabile privind transportul de marfă și a sistemului de gestionare a riscurilor vamale. Acest demers abordează întreaga gamă de riscuri vamale, inclusiv riscurile legate de amenințările la adresa securității și integrității lanțurilor internaționale de aprovizionare și a infrastructurilor critice aferente (de exemplu, amenințările directe, cauzate de importuri, asupra infrastructurilor din porturile maritime, din aeroporturi sau de la frontierele terestre). Îmbunătățirea respectivă are drept scop să garanteze faptul că vămile din UE obțin toate informațiile necesare de la comercianți în privința circulația bunurilor; că aceștia sunt în măsură să transmită cu mai multă eficacitate informații statelor membre; că aplică reguli comune, precum și reguli specifice statului membru, în privința riscurilor, precum și că sunt în măsură să își orienteze cu mai multă eficacitate acțiunile către transporturile riscante, prin ameliorarea cooperării cu alte autorități, în special cu alte agenții de securitate și de aplicare a legii. Eforturile din sectorul tehnologiei informației necesare pentru implementarea acestor îmbunătățiri de către Comisie sunt în etapa inițială, iar investițiile aferente necesare la nivel central vor fi lansate în lunile următoare.

Spatiu

Acțiunea 8: În contextul viitoarei strategii spațiale și a viitorului plan de acțiune european în domeniul apărării, Comisia va propune consolidarea rezilienței infrastructurii spațiale pentru a face față amenințărilor hibride, în special printr-o posibilă extindere a domeniului supravegherii și urmării spațiale pentru a include și amenințările hibride, prin pregătirile pentru integrarea următoarei generații de GovSatCom la nivel european și prin introducerea sistemului Galileo în infrastructurile critice care depind de sincronizarea orei.

La momentul pregătirii, în 2018, a cadrului de reglementare privind comunicarea guvernamentală prin satelit (GovSatCom) și supravegherea și urmărirea spațiale, Comisia va integra în evaluarea sa chestiunile privind reziliența împotriva amenințărilor hibride. În conformitate cu strategia spațială, la momentul elaborării proiectelor privind evoluția sistemelor Galileo și Copernicus, Comisia va evalua potențialul acestor servicii de a ajuta la atenuarea vulnerabilității infrastructurilor critice. Raportul de evaluare ar trebui să fie finalizat în toamna anului 2017, iar propunerea privind următoarea generație de sisteme Copernicus și Galileo va fi prezentată în 2018. Agenția Europeană de Apărare elaborează în prezent proiecte de dezvoltare, pe bază de colaborare, a capacităților în sectoarele comunicațiilor bazate pe

tehnologii spațiale, al poziționării militare, al navigației și sincronizării, precum și al observării Pământului. Toate proiectele se vor concentra asupra cerințelor de reziliență din perspectiva amenințărilor hibride actuale și emergente.

Capabilități de apărare

Acțiunea 9: Înaltul Reprezentant, cu sprijinul statelor membre, după caz, și în colaborare cu Comisia, va propune proiecte privind modul de adaptare a capabilităților de apărare și de dezvoltare a relevanței UE, în special pentru contracararea amenințărilor hibride îndreptate împotriva unuia sau a mai multor state membre.

În 2016 și 2017, Agenția Europeană de Apărare a efectuat trei exerciții de simulare pe calculator privind scenarii de amenințări hibride, împreună cu experți ai Comisiei, ai SEAE și ai statelor membre. Concluziile lor vor servi la revizuirea planului de dezvoltare a capabilităților, astfel încât soluțiile de dezvoltare a capabilităților strategice care vor fi propuse, necesare pentru combaterea amenințărilor hibride, să se numere printre noile priorități ale UE în materie de dezvoltare a capabilităților. Lucrările de revizuire a Catalogului de cerințe din 2005 vor ține seama de dimensiunea amenințărilor hibride. În aprilie 2017, Agenția Europeană de Apărare a finalizat un raport de analiză privind implicațiile militare rezultate în urma unor atacuri hibride dirijate împotriva infrastructurilor portuare critice, care va fi discutat în octombrie 2017, în cadrul unui atelier de lucru cu experți maritimi. O altă analiză specifică privind rolul forțelor militare în combaterea minidronelor este programată pentru 2018. De asemenea, prioritățile în materie de capabilități destinate consolidării rezilienței împotriva amenințărilor hibride identificate de către statele membre ar putea fi, de asemenea, eligibile pentru finanțare prin Fondul european de apărare, începând cu 2019. Comisia invită, pe de o parte, colegislatorii să asigure o adoptare rapidă și, pe de altă parte, statele membre să prezinte propuneri de proiecte de dezvoltare a capabilităților destinate consolidării rezilienței UE împotriva amenințărilor hibride.

Acțiunea 10: Comisia, în cooperare cu statele membre, va îmbunătăți gradul de conștientizare și reziliența la amenințările hibride în cadrul mecanismelor existente de pregătire și coordonare, în special al Comitetului pentru securitate sanitară.

Pentru îmbunătățirea nivelului de pregătire și de reziliență împotriva amenințărilor hibride, inclusiv pentru consolidarea capacităților din cadrul sistemelor de sănătate și a sistemelor alimentare, Comisia sprijină statele membre, prin exerciții de formare și de simulare, precum și prin facilitarea elaborării de orientări pe baza schimbului de experiență și prin finanțarea acțiunilor comune. Aceste acțiuni au loc în special în cadrul sistemului pentru securitate sanitară al UE privind amenințările transfrontaliere grave la adresa sănătății și în cadrul programului din domeniul sănătății publice de implementare a Regulamentului sanitar internațional, un pilon legislativ, obligatoriu în 196 de țări, inclusiv în statele membre, al cărui obiectiv este de a preveni și a răspunde riscurilor transfrontaliere acute pentru sănătatea publică la nivel mondial. Pentru a testa nivelul de pregătire și capacitatea de reacție transectoriale din domeniul sănătății, serviciile Comisiei vor efectua, în toamna anului 2017, un exercițiu privind amenințările hibride complexe și multidimensionale. Comisia și statele membre pregătesc o acțiune comună privind vaccinarea, inclusiv privind previziunile legate de cererea și oferta de vaccinuri și cercetările care se concentrează pe procesele inovatoare de fabricare a vaccinurilor, în scopul de a îmbunătăți furnizarea de vaccinuri și de a ameliora securitatea sanitară la nivelul UE (2018-2020). De asemenea, Comisia colaborează cu Autoritatea Europeană pentru Siguranța Alimentară și cu Centrul European de Prevenire și Control al Bolilor pentru adaptarea la tehnicile avansate de investigație științifică, pentru o

identificare mai precisă a surselor de amenințări la adresa sănătății și, implicit, pentru o gestionare rapidă a focarelor care reprezintă o amenințare pentru siguranța alimentară. Comisia a stabilit o rețea de finanțatori ai activităților de cercetare - Colaborarea la nivel mondial în materie de cercetare pentru pregătire în eventualitatea apariției unor boli infecțioase - pentru a putea reacționa în mod coordonat în domeniul cercetării în termen de 48 de ore de la apariția oricărui focar semnificativ.

Acțiunea 11: Comisia încurajează statele membre, ca o chestiune prioritară, să creeze și să utilizeze pe deplin o rețea formată din 28 CSIRT și CERT-UE (Centrul de răspuns la incidente de securitate cibernetică-UE), precum și un cadru pentru cooperare strategică. Comisia, în coordonare cu statele membre, ar trebui să se asigure că inițiativele sectoriale privind amenințările cibernetică (de exemplu, în sectoarele aviației, energiei, maritim) sunt în concordanță cu capacitățile transsectoriale care fac obiectul Directivei privind securitatea rețelelor și a informației pentru punerea în comun a informațiilor, expertizei și răspunsurilor rapide.

Recentele atacuri cibernetică globale care au utilizat software de tip „ransomware” (cereri de răscumpărare) și software rău-intenționat pentru a dezactiva mii de sisteme informatice au evidențiat încă o dată necesitatea stringentă de a accelera acțiunile de consolidare a rezilienței și securității în UE. După cum s-a anunțat cu ocazia evaluării de la jumătatea perioadei a pieței unice digitale, Comisia și Înalțul Reprezentant evaluează în prezent Strategia de securitate cibernetică a UE din 2013, în special printr-un pachet a cărui adoptare este prevăzută pentru septembrie 2017. Obiectivul va consta în furnizarea unui răspuns transsectorial mai eficace la aceste amenințări, îmbunătățind încrederea în societatea și în economia digitală. De asemenea, acesta va evalua și mandatul ENISA, Agenția UE pentru Securitatea Rețelelor și a Informațiilor, în scopul de a defini rolul acesteia într-un ecosistem schimbat al securității cibernetică. Consiliul European¹³ a salutat intenția Comisiei de a evalua Strategia de securitate cibernetică.

Adoptarea, în iulie 2016, a Directivei privind securitatea cibernetică (Directiva NIS)¹⁴ a reprezentat un pas strategic către consolidarea rezilienței securității cibernetică la nivel european. Directiva stabilește primele norme la nivelul UE privind securitatea cibernetică, îmbunătățește capacitățile de securitate cibernetică și stimulează cooperarea între statele membre. De asemenea, obligă întreprinderilor din sectoarele critice să ia măsuri de securitate corespunzătoare și să notifice orice incident cibernetic grav autorităților naționale relevante. Aceste sectoare includ sectorul energetic, al transporturilor, al apelor, al sănătății, bancar și infrastructura pieței financiare. Piețele online, serviciile de tip cloud computing și motoarele de căutare vor trebui să ia măsuri similare. Implementarea coerentă în diferitele sectoare, precum și la nivel transfrontalier, va fi asigurată de Grupul de cooperare privind serviciile de rețea și de informații (instituit de Comisie în 2016), a cărui sarcină este să evite fragmentarea pieței. În acest context, Directiva privind securitatea cibernetică este considerată a fi cadrul de referință pentru orice inițiative sectoriale în domeniul securității cibernetică. În plus, directiva crează o rețea a echipelor de intervenție în caz de incidente de securitate informatică (CSIRT), care reunește toate părțile interesate relevante. În același timp, Comisia și CERT-UE monitorizează în mod activ peisajul amenințărilor cibernetică și fac schimb de informații cu autoritățile naționale pentru a se asigura că sistemele de tehnologie a informației din instituțiile UE sunt sigure și reziliente la atacuri cibernetică. Incidentul din mai 2017,

¹³ Concluziile Consiliului European din 22-23 iunie 2017.

¹⁴ Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, JO L 194, 19.7.2016, p.1.

declanșat de software-ul WannaCry de tip ransomware a reprezentat pentru rețea prima ocazie de a lansa schimbul operațional de informații și cooperarea prin furnizarea de consiliere. Echipa UE de intervenție în caz de incidente de securitate informatică a colaborat îndeaproape cu Centrul european de combatere a criminalității informatice (EC3) de la Europol, cu echipele de intervenție în caz de incidente de securitate informatică ale țărilor afectate (CSIRTs), cu unitățile de combatere a criminalității informatice și cu parteneri strategici din sector pentru a atenua amenințarea și a acorda sprijin victimelor. Schimbul de rapoarte de situație națională a permis o înțelegere comună a situației la nivelul UE. Această experiență a permis rețelei să își îmbunătățească gradul de preparare în eventualitatea apariției unor noi incidente (de exemplu, „NonPetya”). De asemenea, au fost identificate o serie de provocări, acestea fiind în curs de abordare.

Acțiunea 12: Comisia, în coordonare cu statele membre, va conlucra cu industria, în contextul unui parteneriat contractual public-privat în materie de securitate cibernetică, pentru a dezvolta și testa tehnologii care să protejeze mai bine utilizatorii și infrastructurile împotriva aspectelor cibernetice ale amenințărilor hibride.

În iulie 2016, Comisia, în coordonare cu statele membre, a semnat cu sectorul un parteneriat public-privat contractual (PPPc) pentru securitatea cibernetică, căruia i s-au alocat investiții de până la 450 de milioane EUR în cadrul programului UE de cercetare și inovare Orizont 2020, cu scopul de a pune la punct și a testa tehnologii care să asigure o mai bună protecție a utilizatorilor și a infrastructurilor împotriva amenințărilor cibernetice și hibride. Parteneriatul a prezentat prima agendă de cercetare strategică paneuropeană, care s-a concentrat pe consolidarea rezilienței infrastructurilor critice, precum și a cetățenilor, împotriva atacurilor cibernetice. De asemenea, parteneriatul a îmbunătățit coordonarea între părțile interesate, permițând o creștere a eficienței și a eficacității în proiectele de securitate cibernetică finanțate în cadrul programului Orizont 2020. Parteneriatul este activ, în paralel, în chestiuni legate de certificarea în materie de securitate cibernetică a tehnologiei comunicațiilor și informației, cât și legate de modalități de rezolvare a problemei lipsei acute de profesioniști cu experiență din domeniul securității cibernetice pe piața muncii. Ținând cont de nevoile considerabile din cercetarea civilă și de nivelul ridicat de reziliență necesar în sectorul apărării, Grupul de tehnologie și cercetare pentru sectorul cibernetic al Agenției Europene de Apărare contribuie la eforturile din domeniile de cercetare identificate de Organizația Europeană pentru Securitatea Cibernetică în agenda sa strategică pentru cercetare și inovare.

Acțiunea 13: Comisia va elabora orientări pentru proprietarii de active în cadrul rețelelor inteligente pentru a îmbunătăți securitatea cibernetică a instalațiilor acestora. În contextul inițiativei privind organizarea pieței energiei electrice, Comisia va analiza posibilitatea de a propune „planuri de pregătire cu privire la riscuri” și norme de procedură privind schimbul de informații și asigurarea solidarității între statele membre în timp de criză, inclusiv norme referitoare la metodele de prevenire și de atenuare a atacurilor cibernetice.

În sectorul energetic, Comisia pregătește o strategie sectorială privind securitatea cibernetică, prin lansarea în viitor a unei platforme de experți din sectorul energiei specializați în securitatea cibernetică, cu scopul de a consolida punerea în aplicare a Directivei NIS. O analiză efectuată în februarie 2017 a identificat cele mai bune tehnici disponibile pentru creșterea nivelului de securitate cibernetică al sistemelor de contorizare inteligente care sprijină această platformă. De asemenea, Comisia a creat o platformă online denumită *Centrul UE pentru schimbul de informații privind incidentele și amenințările*, destinat analizelor și distribuirii informațiilor privind amenințările cibernetice și incidentele din sectorul energetic.

Îmbunătățirea rezilienței sectorului financiar față de amenințările hibride

Acțiunea 14: Comisia, în cooperare cu ENISA¹⁵, cu statele membre, cu autoritățile relevante la nivel internațional, european și național, precum și cu instituțiile financiare, va promova și va facilita platformele și rețelele pentru schimbul de informații privind amenințările și va aborda factorii care împiedică schimbul de astfel de informații.

Recunoscând faptul că amenințările cibernetice se numără printre cele mai mari riscuri la adresa stabilității financiare, Comisia a revizuit cadrul de reglementare privind serviciile de plată din Uniunea Europeană, care este în curs de punere în aplicare în prezent. Directiva revizuită privind serviciile de plată¹⁶ a introdus noi dispoziții pentru a îmbunătăți securitatea serviciilor de plată și autentificarea strictă a clienților, cu scopul de a reduce fraudele, în special la efectuarea plăților online. Noul cadrul legislativ va fi aplicabil începând cu ianuarie 2018. În prezent, Comisia elaborează, cu sprijinul Autorității bancare europene și al părților interesate, standarde tehnice de reglementare privind autentificarea strictă a clienților și comunicarea securizată pentru a asigura efectiv securitatea operațiunilor de plată; aceste standarde ar urma să fie publicate până la sfârșitul anului 2017. De asemenea, pe plan internațional, Comisia a colaborat îndeaproape cu partenerii G7 la elaborarea principiilor fundamentale ale securității cibernetice în sectorul financiar ale G7 (*G7 fundamental principles of cyber security in the financial sector*), aprobate în octombrie 2016 de miniștrii de finanțe și de guvernatorii băncilor centrale ai G7. Principiile sunt concepute pentru entitățile din sectorul financiar (privat și public) și contribuie la o abordare coordonată a securității cibernetice în cadrul sectorului financiar pentru a combate în comun amenințările cibernetice, în particular ținând seama de multiplicarea și de sporirea gradului de sofisticare ale acestora.

Transport

Acțiunea 15: Comisia și Înaltul Reprezentant (în domeniile lor de competență respective), în coordonare cu statele membre, vor examina modalitățile de a răspunde la amenințările hibride, în special în ceea ce privește amenințările legate de atacurile cibernetice în sectorul transporturilor.

Implementarea planului de acțiune privind Strategia UE în materie de securitate maritimă¹⁷ va ajuta la schimbarea mentalității compartimentate în privința schimbului de informații și al utilizării comune a resurselor de către autoritățile civile și militare. Un demers care a inclus întreaga administrație a avut drept efect stimularea cooperării între diferiți actori. O agendă comună de cercetare strategică din domeniile civil și militar a Comisiei și a SEAE ar urma să fie finalizată până la finele anului 2017, conform planificării, urmând să se încheie printr-un atelier privind protecția infrastructurii maritime critice. Aceste lucrări ar putea fi extinse în viitor pentru a aborda amenințările emergente din afara apelor teritoriale asupra conductelor submarine, transferului de energie, fibrelor optice și cablurilor de comunicații tradiționale.

¹⁵ Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor.

¹⁶ Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, JO L 337, 23.12.2015, p. 35.

¹⁷ https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf și cel de-al doilea raport privind implementarea SUESM prezentat statelor membre la 21 iunie 2017.

Un studiu recent¹⁸ a examinat capacitatea de evaluare a riscurilor de către autoritățile naționale care îndeplinesc un rol de gardă de coastă. Acesta a identificat cele mai importante obstacole din calea colaborării și a recomandat modalități practice de a îmbunătăți cooperarea dintre autoritățile maritime de la nivelul UE și de la nivel național în acest domeniu specific. Evaluarea riscurilor este esențială pentru combaterea amenințărilor maritime; aceasta este și mai determinantă pentru evaluarea și prevenirea amenințărilor hibride, întrucât aceste amenințări necesită considerații suplimentare, mai complexe. Rezultatele acestui studiu vor fi prezentate diferitelor forumuri cu legătură cu gărzile de coastă, astfel încât recomandările propuse să poată fi evaluate și implementate pentru a spori cooperarea în acest domeniu, având drept obiective prioritare gradul de pregătire și răspunsul la amenințările hibride.

Combaterea finanțării terorismului

Acțiunea 16: Comisia va utiliza punerea în aplicare a Planului de acțiune privind finanțarea terorismului pentru a contribui, de asemenea, la contracararea amenințărilor hibride.

Autorii amenințărilor hibride și partizanii acestora au nevoie de finanțare pentru a-și pune în aplicare planurile. Eforturile depuse de UE pentru combaterea finanțării criminalității și a terorismului în cadrul Agendei privind securitatea și al Planului de acțiune pentru combaterea finanțării terorismului pot, de asemenea, să contribuie la combaterea amenințărilor hibride. În decembrie 2016, Comisia a prezentat trei propuneri legislative, inclusiv privind introducerea de sancțiuni penale în cazul spălării de bani și a plăților ilicite în numerar, precum și privind înghețarea și confiscarea bunurilor¹⁹.

Toate statele membre trebuie să transpună cea de-a patra Directivă privind combaterea spălării banilor²⁰ până la 26 iunie 2017; în iulie 2016, Comisia a prezentat o propunere legislativă orientată pentru a completa și a consolida directiva menționată mai sus cu măsuri suplimentare²¹.

La 26 iunie 2016, Comisia a publicat evaluarea riscurilor supranaționale prevăzută de a patra Directivă privind combaterea spălării banilor. De asemenea, Comisia a prezentat o propunere de regulament al cărui scop este de a preveni importul și stocarea în UE a bunurilor culturale exportate ilegal din țări terțe²². Ulterior, în cursul acestui an, Comisia va raporta, în cadrul evaluării sale în curs de desfășurare, asupra necesității de a impune posibile măsuri suplimentare pentru a depista finanțările teroriste din UE. De asemenea, Comisia revizuieste

¹⁸ Studiu intitulat „*Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions* (Evaluarea capacității de evaluare a riscurilor la nivelul autorităților statelor membre care îndeplinesc funcții de gardă de coastă)”, 2017, <https://ec.europa.eu/maritimeaffairs/documentation/studies>

¹⁹ Al treilea raport cu privire la progresele înregistrate pentru realizarea unei Uniuni a securității efective și reale [COM(2016) 831 final].

²⁰ Directiva (UE) 2015/849 a Parlamentului European și a Consiliului din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului și de abrogare a Directivei 2005/60/CE a Parlamentului European și a Consiliului și a Directivei 2006/70/CE a Comisiei (text cu relevanță pentru SEE), JO L 141, 5.6.2015, p. 73-117.

²¹ Pentru detalii suplimentare puteți consulta Al treilea raport cu privire la progresele înregistrate pentru realizarea unei Uniuni a securității efective și reale [COM(2016) 831 final] și Al optulea raport cu privire la progresele înregistrate pentru realizarea unei Uniuni a securității efective și reale [COM(2017) 354 final].

²² COM(2017) 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final 0.

în prezent legislația privind combaterea fraudelor și a falsificării mijloacelor de plată altele decât numerarul²³.

Al optulea raport cu privire la progresele înregistrate pentru realizarea unei Uniuni a securității efective și reale oferă detalii suplimentare privind situația implementării planului de acțiune împotriva finanțării terorismului.

Promovarea valorilor comune ale UE și a unor societăți favorabile incluziunii, deschise și reziliente

Dezvoltarea rezilienței împotriva radicalizării și a extremismului violent

Radicalizarea religioasă și ideologică, conflictele etnice și conflictele cu minoritățile pot fi stimulate de actori externi prin intermediul sprijinului acordat unor grupuri specifice sau prin eforturile depuse pentru a promova conflictele în rândul diferitelor grupuri. Au apărut noi provocări, precum amenințările unor actori izolați, noi modele de radicalizare, inclusiv, potențial, în contextul crizei migrației, cât și ascensiunea extremismului de dreapta (inclusiv violența împotriva migranților) și riscurile de polarizare. În timp ce eforturile împotriva radicalizării continuă în contextul uniunii securității, acestea pot fi relevante în mod indirect din punctul de vedere al amenințărilor hibride în sensul în care persoanele vulnerabile la radicalizare pot fi manipulate de autori ai amenințărilor hibride.

Acțiunea 17: Comisia pune în aplicare acțiunile de combatere a radicalizării prevăzute în Agenda europeană privind securitatea și analizează necesitatea de a consolida procedurile pentru eliminarea conținutului ilegal, solicitând intermediarilor să-și exercite obligația de diligență în gestionarea rețelelor și sistemelor.

Prevenirea radicalizării

Comisia continuă să ofere un răspuns multidimensional la radicalizare, astfel cum a fost stabilit în Comunicarea sa din iunie 2016 privind sprijinirea prevenirii radicalizării care duce la extremism violent²⁴, prin acțiuni strategice precum promovarea educației incluzive și a valorilor comune, lupta împotriva propagandei extremiste online și împotriva radicalizării din mediul carceral, întărirea cooperării cu țările terțe și intensificarea cercetării pentru o mai bună înțelegere a naturii evolutive a radicalizării și o informare mai clară în vederea formulării răspunsurilor politice. Rețeaua pentru sensibilizarea publicului cu privire la radicalizare (RAN) s-a situat în primul plan al acțiunilor Comisiei de sprijinire a statelor membre în acest domeniu, colaborând cu actorii locali de la nivelul comunităților. Pentru detalii suplimentare puteți consulta Al optulea raport cu privire la progresele înregistrate pentru realizarea unei uniuni a securității efective și reale²⁵.

Radicalizare și discurs de incitare la ură online

²³ Al optulea raport cu privire la progresele înregistrate pentru realizarea unei Uniuni a securității efective și reale [COM(2017) 354 final].

²⁴ http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf

²⁵ COM(2017) 354 final.

În conformitate cu Agenda europeană privind securitatea²⁶, Comisia a întreprins măsuri pentru a reduce disponibilitatea conținutului ilegal online, în special prin intermediul Unității UE de semnalare a conținutului online de la Europol și al Forumului pentru internet al UE²⁷. De asemenea, s-au înregistrat progrese remarcabile în cadrul codului de conduită pentru a lupta împotriva discursurilor ilegale de incitare la ură²⁸. Pentru detalii suplimentare, puteți consulta Al optulea raport cu privire la progresele înregistrate pentru realizarea unei uniuni a securității efective și reale²⁹. Aceste acțiuni vor fi consolidate, în conformitate, de asemenea, cu concluziile Consiliului European³⁰, cu reuniunea la vârf a G7³¹ și cu reuniunea la vârf de la Hamburg a G20³².

Platformele online au un rol vital în combaterea conținutului ilegal sau potențial periculos. În conformitate cu Strategia privind piața unică digitală, astfel cum este stabilit în revizuirea de la jumătatea perioadei³³, Comisia va asigura o mai bună coordonare a dialogurilor cu platformele, privilegiind mecanismele și soluțiile tehnice pentru eliminarea conținutului ilegal. După caz, obiectivul ar trebui să fie sprijinirea acestor mecanisme prin orientări privind aspecte precum notificarea și eliminarea conținutului ilegal. Comisia va formula, de asemenea, orientări privind regulile în materie de responsabilitate.

Îmbunătățirea cooperării cu țările terțe

Acțiunea 18: Înalțul Reprezentant, în coordonare cu Comisia, va lansa un studiu privind riscurile hibride în regiunile învecinate. Înalțul Reprezentant, Comisia și statele membre vor utiliza instrumentele aflate la dispoziția lor pentru consolidarea capacităților partenerilor și consolidarea rezilienței acestora la amenințările hibride. Ar putea fi desfășurate misiuni PSAC, în mod independent sau pentru a completa instrumentele UE, care să sprijine partenerii în ceea ce privește consolidarea capacităților acestora.

Uniunea Europeană pune în prezent un accent sporit pe dezvoltarea capacităților și a rezilienței țărilor partenere în domeniul securității, prin valorificarea legăturii dintre securitate și dezvoltare, consolidând dimensiunea „securitate” a politicii europene de vecinătate și angajând dialoguri în materie de antiterorism și de securitate cu țările din bazinul mediteranean. În acest sens, a fost lansat un studiu privind riscurile, în cadrul unui proiect-pilot, în cooperare cu Republica Moldova. Obiectivul acestuia este de a identifica principalele vulnerabilități ale țării și de a se asigura că asistența UE vizează în mod specific domeniile respective. Rezultatele proiectului-pilot au demonstrat că studiul în sine a fost considerat util. Pe baza experienței acumulate, Comisia și SEAE vor formula recomandări privind prioritatea

²⁶ Pentru detalii suplimentare, puteți consulta Al optulea raport cu privire la progresele înregistrate pentru realizarea unei Uniuni a securității efective și reale [COM(2017) 354 final]

²⁷ Pentru detalii suplimentare, puteți consulta Al optulea raport cu privire la progresele înregistrate pentru realizarea unei Uniuni a securității efective și reale [COM(2017) 354 final]

²⁸ Codul de conduită privind discursurile ilegale de incitare la ură din mediul online, 31 mai 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

²⁹ Pentru detalii suplimentare, puteți consulta Al optulea raport cu privire la progresele înregistrate pentru realizarea unei Uniuni a securității efective și reale [COM(2017) 354 final]

³⁰ Concluziile Consiliului, 22-23 iunie 2017.

³¹ Reuniunea la vârf a G7 de la Taormina, Italia, 26-27.5.2017.

³² Reuniunea la vârf a G20 de la Hamburg, Germania, 7-8.7.2017.

³³ Cf. Comunicarea de mai sus a Comisiei COM(2017) 228 final.

care ar trebui acordată acțiunilor corespunzătoare capitolului „Eficacitate, comunicații strategice, protecția infrastructurilor critice și securitate cibernetică”.

În viitor, ar putea beneficia de acest studiu și alte țări vecine, pornind de la această primă experiență, cu condiția efectuării unor adaptări care să reflecte situațiile locale diferite și amenințările specifice și cu condiția de a evita suprapunerea acțiunilor cu dialogurile în curs de desfășurare privind antiterorismul și securitatea. Pe plan mai general, la 7 iunie 2017, Comisia și Înalțul Reprezentant au adoptat o Comunicare comună privind „O abordare strategică a rezilienței în cadrul acțiunii externe a UE”³⁴. Obiectivul este de a ajuta țările partenere în eforturile lor de a-și consolida reziliența în fața provocărilor globale actuale. Această comunicare recunoaște necesitatea de a trece de la o abordare de izolare a crizei la o abordare mai structurală, pe termen lung, a vulnerabilităților, punând accentul pe anticipare, prevenire și pe gradul de pregătire.

Reziliența cibernetică pentru dezvoltare

UE sprijină țări din afara Europei pentru a-și consolida reziliența rețelelor de informații. Digitalizarea tot mai amplă are o dimensiune de securitate implicită care prezintă numeroase provocări specifice la adresa rezilienței sistemelor de rețele de informații la scară globală, întrucât atacurile ciberneticе nu au frontiere. UE ajută țările terțe să își consolideze capacitatea de a preveni în mod corespunzător și de a reacționa la defecțiunile accidentale și la atacurile ciberneticе. În urma unui proiect-pilot desfășurat în fosta Republică iugoslavă a Macedoniei, în Kosovo³⁵ și în Moldova și încheiat în 2016, Comisia va lansa un nou program pentru a îmbunătăți reziliența țărilor terțe, în principal în Africa și Asia, dar și în Ucraina, pentru perioada 2017-2020. Programul are scopul de a spori securitatea și gradul de pregătire al infrastructurilor și rețelelor critice de informație în țările terțe pe baza unei abordări la nivelul întregii administrații, asigurând în același timp garantarea drepturilor omului și a statului de drept.

Securitatea aeronautică

Aviația civilă rămâne o țintă principală și simbolică pentru teroriști, dar ar putea deveni și ținta unei campanii hibride. Deși UE a pus la punct un cadru solid al securității aeronautice, zborurile provenind din țări terțe pot fi mai vulnerabile. În conformitate cu rezoluția 2309 (2016) a Consiliului de Securitate al ONU, Comisia își intensifică eforturile de consolidare a capacităților din țări terțe. În ianuarie 2017, Comisia a lansat o nouă evaluare integrată a riscurilor pentru a ierarhiza și a coordona eforturile în domeniul îmbunătățirii capacităților la nivelul UE și la nivelul statelor membre, precum și cu partenerii internaționali. În 2016, Comisia a lansat un proiect cvadrienal privind securitatea aviației civile în Africa și în Peninsula Arabică pentru a lupta împotriva amenințărilor de terorism îndreptate împotriva aviației civile. Proiectul este axat pe schimbul de experiență între statele membre și experți din statele membre ai Conferinței Europene a Aviației Civile, precum și pe tutorat, formare, activități de îndrumare. Activitățile se vor extinde în continuare în 2017.

³⁴Comunicare comună către Parlamentul European și Consiliu: O abordare strategică a rezilienței în cadrul acțiunii externe a UE JOIN(2017) 21 final.

³⁵ Această denumire nu aduce atingere pozițiilor privind statutul și este conformă cu RCSONU 1244, precum și cu Avizul CIJ privind Declarația de independență a Kosovo.

c. PREVENIREA CRIZELOR, REACȚIA LA CRIZE ȘI REDRESAREA

Deși consecințele pot fi atenuate prin politici pe termen lung la nivel național și la nivelul UE, pe termen scurt este esențială consolidarea capacității statelor membre și a Uniunii de a preveni, a răspunde și a se redresa după amenințările hibride, în mod rapid și coordonat. O reacție rapidă la evenimentele declanșate de amenințările hibride este primordială. În cursul anului trecut, au fost înregistrate progrese importante în acest domeniu, iar în prezent există un protocol operațional care definește procesul de gestionare a crizelor în cazul unui atac hibrid. Supravegherea și exercițiile vor continua în mod periodic.

Acțiunea 19: Înaltul Reprezentant și Comisia, în coordonare cu statele membre, vor stabili un protocol operațional comun și vor efectua exerciții periodice pentru a îmbunătăți capacitatea de luare a deciziilor strategice ca răspuns la amenințările hibride complexe pe baza procedurilor de gestionare a crizelor și a mecanismului integrat al UE pentru un răspuns politic la crize.

Cadrul comun a recomandat stabilirea unor mecanisme de reacție rapidă la evenimentele declanșate de amenințări hibride, care să fie coordonate cu mecanismele de reacție³⁶ și cu sistemele de alertă timpurie ale UE. În acest scop, serviciile Comisiei și SEAE au pus la punct protocolul operațional al UE de combatere a amenințărilor hibride (*EU Playbook*)³⁷, care precizează modalitățile de coordonare, de fuzionare și analiză a informațiilor, de participare la sistemul de luare a deciziilor, de efectuare a exercițiilor și a formării și de cooperare cu organizațiile partenere, în special cu NATO, în cazul unei amenințări hibride. În mod similar, NATO a elaborat un protocol pentru o cooperare mai strânsă NATO-UE în scopul prevenirii și combaterii amenințărilor comune în domeniile apărării cibernetice, al comunicațiilor strategice, al gradului de cunoaștere a situației și al managementului crizelor. Protocolul operațional al UE pentru combaterea amenințărilor hibride va fi testat, în toamna anului 2017, în cadrul exercițiului paralel și coordonat al Uniunii Europene, care include interacțiunea cu NATO.

Acțiunea 20: Comisia și Înaltul Reprezentant vor examina, în domeniile lor de competență respective, aplicabilitatea și implicațiile practice ale articolului 222 din TFUE și ale articolului 42 alineatul (7) din TUE în cazul în care are loc un atac hibrid de mare amploare și grav.

Articolul 42 alineatul (7) din TUE se referă la o agresiune armată pe teritoriul unui stat membru, iar articolul 222 din TFUE (clauza de solidaritate) se referă la un atac terorist sau la o catastrofă provocată de om pe teritoriul unui stat membru. În cazul atacurilor hibride, care se caracterizează printr-o combinație de acțiuni criminale/subversive, este mai probabilă invocarea celui din urmă articol. Invocarea clauzei de solidaritate declanșează coordonarea la nivelul Consiliului (Mecanismul integrat pentru un răspuns politic la criză, IPCR) și implicarea instituțiilor, agențiilor și organismelor relevante ale UE, precum și a programelor și mecanismelor de asistență ale UE. Decizia 2014/415/UE a Consiliului prevede modalitățile de punere în aplicare de către Uniune a clauzei de solidaritate. Aceste modalități de aplicare rămân valabile și nu este nevoie de o revizuire a deciziei Consiliului. În cazul în care un atac hibrid include o agresiune armată, poate fi invocat, de asemenea, articolul 42 alineatul (7). Într-o astfel de situație, ajutorul și asistența sunt acordate atât de statul membru, cât și de UE.

³⁶ Mecanismul integrat al UE pentru un răspuns politic la crize coordonat de Consiliu (IPCR), Sistemul ARGUS al Comisiei și Mecanismul de reacție la crize (CRM) al SEAE.

³⁷ Document de lucru al Comisiei (2016) 227 adoptat la 7 iulie 2016.

Comisia și Înalțul Reprezentant vor continua să evalueze cele mai eficace modalități de a face față unor astfel de atacuri.

Protocolul operațional al UE, menționat mai sus, contribuie direct la această evaluare; acesta va fi pus în practică în octombrie 2017 în cadrul exercițiului paralel și coordonat al UE (PACE). Acest exercițiu va testa diferitele mecanisme ale UE și capacitatea de interacțiune a UE, scopul fiind de a accelera procesul decizional atunci când ambiguitatea creată de un atac hibrid afectează claritatea.

Acțiunea 21: Înalțul Reprezentant, în coordonare cu statele membre, va integra, exploata și coordona capacitățile acțiunii militare în contracararea amenințărilor hibride în temeiul politicii de securitate și apărare comune.

Drept răspuns la misiunea de integrare a capacităților militare în scopul sprijinirii PESC/PSAC, avizul militar privind documentul intitulat „EU military contribution to countering hybrid threats within the CSDP (Contribuția militară a UE la contracararea amenințărilor hibride în cadrul PSAC)” a fost finalizat în iulie 2017, în urma unui seminar comun cu experți militari, care a avut loc în decembrie 2016, și a orientărilor primite în mai 2016 de la Comitetul militar al Uniunii Europene. Acest aviz va fi aplicat în mod concret în cadrul planului de punere în aplicare a elaborării conceptelor.

d. COOPERAREA UE-NATO

Acțiunea 22: Înalțul Reprezentant, în coordonare cu Comisia, va continua dialogul informal și intensificarea cooperării și coordonării cu NATO cu privire la gradul de cunoaștere a situației, comunicările strategice, securitatea cibernetică, prevenirea crizelor și reacția la crize în vederea contracarării amenințărilor hibride, respectând principiile incluziunii și autonomiei procesului decizional al fiecărei organizații.

Pe baza declarației comune semnate la 8 iulie 2016, la Varșovia, de președinții Consiliului European și al Comisiei Europene, precum și de secretarul general al NATO, UE și NATO au elaborat un set comun de 42 de propuneri de punere în aplicare, care a fost ulterior aprobat la 6 decembrie 2016, în procese paralele distincte, de către Consiliile respective al UE și al NATO³⁸. În iunie 2017, Înalțul Reprezentant/vicepreședintele și secretarul general al NATO au publicat un raport privind situația punerii în aplicare a celor 42 de acțiuni din declarația comună. Contracararea amenințărilor hibride este unul dintre cele 7 domenii de cooperare identificate în declarația comună, incluzând 10 dintre cele 42 de acțiuni. Raportul demonstrează că eforturile comune depuse de-a lungul ultimului an au permis obținerea unor rezultate substanțiale. Multe dintre acțiunile specifice destinate contracarării acțiunilor hibride au fost deja menționate, inclusiv instituirea Centrului European de Excelență pentru Contracararea Amenințărilor Hibride, o mai bună cunoaștere a situației, instituirea celulei de fuziune a UE împotriva amenințărilor hibride și interacțiunea acesteia cu noul departament de analiză a amenințărilor hibride al NATO și colaborarea dintre echipele de comunicare strategică. Pentru prima oară, personalul NATO și cel al UE vor efectua împreună un exercițiu destinat testării reacției lor la un scenariu de amenințare hibridă. Acest exercițiu ar urma să testeze punerea în aplicare a mai mult de o treime din setul de propuneri comune. UE va efectua, în acest an, propriul său exercițiu paralel și coordonat și se pregătește să joace un rol de lider în 2018.

³⁸ <http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/>

În ceea ce privește reziliența, personalul UE și cel al NATO au început organizarea unor sesiuni de informare încrucișată, cu tematici precum mecanismul integrat al UE pentru un răspuns politic la crize. Comunicarea periodică între personalul NATO și cel al UE, de exemplu prin intermediul atelierelor sau prin participarea NATO la Comitetul director al Agenției Europene de Apărare, a permis efectuarea schimbului de informații privind cerințele de bază ale NATO în privința rezilienței naționale. Pentru această toamnă, sunt prevăzute noi schimburi de informații între Comisie și NATO privind modalitățile de consolidare a rezilienței. Următorul raport intermediar privind cooperarea UE-NATO va propune posibilități de extindere a cooperării dintre cele două organizații.

3. CONCLUZIE

Cadrul comun prezintă acțiunile concepute pentru a sprijini combaterea amenințărilor hibride și a favoriza reziliența la nivelul UE, la scară națională și la nivelul partenerilor. Comisia și Înalțul Reprezentant obțin deja rezultate în toate domeniile, în strânsă colaborare cu statele membre și cu partenerii, însă este esențială menținerea acestei dinamici pentru a face față amenințărilor hibride persistente și în continuă evoluție. Responsabilitatea principală a luptei împotriva amenințărilor hibride legate de securitatea națională și de menținerea ordinii publice le revine statelor membre. Reziliența națională și eforturile colective depuse pentru a se proteja împotriva amenințărilor hibride trebuie văzute ca elemente ale unui demers global unitar, care se consolidează reciproc. Prin urmare, statele membre sunt încurajate să efectueze, cât mai rapid posibil, studii asupra riscurilor hibride, întrucât acestea vor furniza informații valoroase privind gradul de vulnerabilitate și de pregătire la nivel european. Pe baza progreselor semnificative realizate în ceea ce privește cunoașterea situației, ar trebui exploatat la maximum potențialul celulei de fuziune a UE împotriva amenințărilor hibride. Înalțul Reprezentant invită statele membre să sprijine activitatea grupurilor operative StratCom pentru a contracara mai eficient tendința de creștere a amenințărilor hibride. UE va susține pe deplin Centrul European pentru Contracarea Amenințărilor Hibride, coordonat de Finlanda.

Atuul unic al UE constă în sprijinul acordat statelor membre și partenerilor pentru a-și consolida reziliența, pe baza unei game largi de instrumente și programe existente. Acțiunile realizate pentru consolidarea rezilienței se bucură de succes în domenii precum transporturile, energia, securitatea cibernetică, infrastructura critică, protecția sistemului financiar împotriva utilizării ilegale și eforturile de contracarare a extremismului violent și a radicalizării. Acțiunile UE pentru consolidarea rezilienței vor continua, întrucât natura amenințărilor hibride evoluează. În special, UE va pregăti indicatori pentru a îmbunătăți protecția și reziliența infrastructurilor critice împotriva amenințărilor hibride în sectoarele relevante.

Fondul european de apărare poate cofinanța, împreună cu statele membre, capacitățile considerate prioritare în scopul de a îmbunătăți reziliența împotriva amenințărilor hibride. Pachetul de măsuri anunțat privind securitatea cibernetică, precum și măsurile transsectoriale destinate punerii în aplicare a Directivei privind securitatea rețelelor și a informațiilor vor prevedea noi platforme de combatere a amenințărilor hibride în UE.

Comisia și Înalțul Reprezentant invită statele membre și părțile interesate, după caz, să ajungă în cel mai scurt timp la un acord și să asigure punerea în aplicare rapidă și eficace a numeroaselor măsuri destinate îmbunătățirii rezilienței, descrise în prezenta comunicare. UE va consolida și va aprofunda cooperarea, deja fructuoasă, pe care a început-o cu NATO.

Uniunea este în continuare hotărâtă să mobilizeze toate instrumentele relevante ale UE pentru a face față amenințărilor hibride complexe. Sprijinirea eforturilor statelor membre rămâne o prioritate pentru Uniune, care acționează ca un garant al securității mai puternic și mai dinamic, alături de principalii săi parteneri.