Consiliul
Uniunii Europene

Bruxelles, 18 iunie 2018
(OR. en)

10242/18

HYBRID 11	**ENER 242**
COPS 223	**EUMC 106**
PROCIV 40	**CIVCOM 120**
CSDP/PSDC 346	**TRANS 271**
CYBER 147	**COEST 126**
CFSP/PESC 583	**ESPACE 32**
JAI 668	**COTER 80**
ECOFIN 632	**CSC 200**
POLMIL 89	**IPCR 15**

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretar general al Comisiei Europene, sub semnătura dlui Jordi AYET PUIGARNAU, director
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	JOIN(2018) 16 final
Subiect:	COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN, CONSILIUL EUROPEAN ȘI CONSILIU Creșterea rezilienței și consolidarea capacităților necesare pentru a aborda amenințările hibride

În anexă, se pune la dispoziția delegațiilor documentul JOIN(2018) 16 final.

Anexă: JOIN(2018) 16 final

COMISIA
EUROPEANĂ

ÎNALTUL REPREZENTANT AL
UNIUNII PENTRU AFACERI
EXTERNE ȘI POLITICA
DE SECURITATE

Bruxelles, 13.6.2018
JOIN(2018) 16 final

COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN, CONSILIUL EUROPEAN ȘI CONSILIU

Creșterea rezilienței și consolidarea capacităților necesare pentru a aborda amenințările hibride

1. INTRODUCERE

Activitățile hibride desfășurate de actori statali și nestatali continuă să reprezinte o amenințare acută și gravă pentru UE și pentru statele sale membre. Eforturile de a destabiliza țări prin subminarea încrederii publicului în instituțiile guvernamentale și prin contestarea valorilor fundamentale ale societăților au devenit mai frecvente. Societățile noastre se confruntă cu o provocare gravă din partea celor care urmăresc să cauzeze un prejudiciu Uniunii Europene și statelor sale membre, de la atacuri informatice care afectează economia și serviciile publice, trecând prin campanii de dezinformare selectivă și până la acțiuni militare ostile.

Campaniile hibride sunt multidimensionale, combinând măsuri coercitive și subversive, utilizând atât instrumente și tactici convenționale, cât și unele neconvenționale (diplomatice, militare, economice și tehnologice) pentru a destabiliza adversarul. Acestea sunt concepute pentru a fi dificil de detectat sau atribuit și pot fi utilizate atât de actori statali, cât și de actori nestatali. Atacul cu agent neurotoxic de la Salisbury din luna martie[1] a evidențiat în continuare versatilitatea amenințărilor hibride și multitudinea tacticilor disponibile în prezent. Ca răspuns, Consiliul European[2] a subliniat necesitatea de a consolida capacitatea UE și a statelor sale membre de a detecta, a preveni și a răspunde amenințărilor hibride în domenii precum securitatea cibernetică, comunicarea strategică și contrainformațiile. De asemenea, Consiliul a atras atenția în special asupra necesității unei capacități de reziliență în fața amenințărilor chimice, biologice, radiologice și nucleare.

Amenințările reprezentate de armele neconvenționale alcătuiesc o categorie proprie din cauza amplorii potențiale a daunelor pe care le pot provoca acestea. Pe lângă faptul că acestea sunt dificil de detectat și atribuit, remedierea lor reprezintă o chestiune complexă. Amenințările chimice, biologice, radiologice și nucleare, care depășesc amenințările hibride și cuprind, de asemenea, amenințările teroriste, reprezintă, la rândul lor, o preocupare generală a comunității internaționale[3], în special în ceea ce privește riscul de proliferare care evoluează atât pe plan geografic, cât și la nivelul actorilor nestatali.

Consolidarea rezilienței la aceste amenințări și îmbunătățirea capacităților constituie, în principal, responsabilitatea statelor membre. Cu toate acestea, instituțiile UE au luat deja o serie de măsuri pentru a contribui la consolidarea eforturilor naționale. Acestea au inclus acțiuni desfășurate în strânsă colaborare cu alți actori internaționali, în special Organizația Tratatului Atlanticului de Nord (NATO)[4], iar astfel de activități ar putea fi aprofundate în continuare sub forma sprijinului acordat statelor membre în domenii precum răspunsul rapid[5].

Prezenta comunicare comună vine ca răspuns la invitația Consiliului European de a continua aceste demersuri. Aceasta face parte dintr-un pachet mai amplu, care include, de

---

1 În ceea ce privește atacul de la Salisbury, Consiliul European din 22 martie 2018 „este de acord cu evaluarea Guvernului Regatului Unit potrivit căreia este foarte probabil ca Federația Rusă să fie responsabilă de atac și cu faptul că nu există o altă explicație plauzibilă".

2 Concluziile Consiliului European din martie 2018.

3 Exprimată inclusiv de Consiliul de Securitate al Organizației Națiunilor Unite, Rezoluția S/RES/2325 (2016), 14 decembrie 2016.

4 Contracararea amenințărilor hibride este unul dintre cele șapte domenii de cooperare cu Organizația Tratatului Atlanticului de Nord, prezentate în declarația comună semnată la Varșovia în iulie 2016 de către președintele Consiliului European, președintele Comisiei Europene și secretarul general al Organizației Tratatului Atlanticului de Nord.

5 Liderii G7, care s-au reunit la summitul de la Charlevoix din iunie 2018, au convenit, de asemenea, să dezvolte un mecanism de răspuns rapid al G7 pentru a aborda amenințările la adresa democrațiilor: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

asemenea, cel mai recent raport privind progresele înregistrate către o uniune a securității[6], care trece în revistă și prezintă următoarele etape în punerea în aplicare a Planului de acțiune privind riscurile de siguranță chimică, biologică, radiologică și nucleară din octombrie 2017[7], precum și cel de al doilea raport privind progresele înregistrate[8] cu privire la punerea în aplicare a celor 22 de acțiuni din Cadrul comun privind contracararea amenințărilor hibride – un răspuns al Uniunii Europene[9].

2. RĂSPUNSUL UE

Comisia și Înaltul Reprezentant au depus eforturi consecvente pentru consolidarea capacităților UE și pentru a sprijini în mod eficace statele membre în a combate amenințările hibride și amenințările chimice, biologice, radiologice și nucleare. S-au obținut deja rezultate tangibile în domenii precum comunicările strategice, conștientizarea situației, consolidarea nivelului de pregătire și de reziliență și consolidarea capacității de reacție în situații de criză.

Grupul operativ East Stratcom, înființat după Consiliul European din martie 2015, a coordonat activitatea pentru prognozarea, urmărirea și combaterea dezinformării provenind din surse străine. Analizele realizate de experți și produsele publice[10] ale acestuia au crescut semnificativ gradul de conștientizare cu privire la impactul dezinformării ruse. În ultimii doi ani, acesta a identificat peste 4 000 de cazuri individuale de dezinformare, dintre care multe vizează în mod deliberat Europa. Activitatea grupului operativ East Stratcom s-a concentrat, de asemenea, pe îmbunătățirea difuzării de comunicări pozitive, cu îmbunătățirea accesului în vecinătatea estică. În urma acestui succes, au fost create încă două grupuri operative cu accent geografic diferit – un grup operativ pentru Balcanii de Vest și un grup operativ specific pentru zona sudică vizând lumea arabă.

Au fost luate măsuri importante pentru a construi structurile necesare în scopul de a îmbunătăți conștientizarea situației și de a sprijini procesul decizional. Celula de fuziune împotriva amenințărilor hibride a fost instituită în 2016 în cadrul Centrului de situații și de analiză a informațiilor al UE care face parte din Serviciul European de Acțiune Externă. Celula de fuziune primește și analizează informațiile clasificate și din surse deschise privind amenințările hibride provenind de la diferite părți interesate. Până în prezent, s-au elaborat peste 100 de evaluări și note de informare, partajate la nivelul UE și între statele membre pentru a contribui la procesul decizional al UE. Celula de fuziune împotriva amenințărilor hibride are o strânsă relație de cooperare cu Centrul European de Excelență pentru Contracararea Amenințărilor Hibride de la Helsinki. Înființat în aprilie 2017 pentru a încuraja dialogul strategic și pentru a efectua cercetări și analize privind amenințările hibride, centrul și-a mărit până în prezent numărul de membri la 16 țări[11] și beneficiază de sprijin susținut din partea UE.

---

6 Al cincisprezecelea raport privind progresele înregistrate către o uniune a securității efectivă și reală, COM(2018) 470.

7 COM(2017) 610 final.

8 Raport comun privind punerea în aplicare a cadrului comun privind contracararea amenințărilor hibride (iulie 2017 – iulie 2018), JOIN(2018) 14.

9 JOIN(2016) 18 final.

10 A se vedea www.euvsdisinfo.eu

11 Dintre cei 16 membri actuali, 14 sunt state membre ale UE: Republica Cehă, Danemarca, Estonia, Finlanda, Franța, Italia, Germania, Letonia, Lituania, Țările de Jos, Polonia, Spania, Suedia, Regatul Unit. Inițiativa pentru crearea acestuia își are originea în Cadrul comun privind contracararea amenințărilor hibride. De asemenea, centrul a fost sprijinit în mod activ de UE și de Organizația Tratatului Atlanticului de Nord în cadrul cooperării acestora.

De asemenea, s-au luat măsuri importante pentru consolidarea pregătirii și a reziliență, în special împotriva amenințărilor chimice, biologice, radiologice și nucleare. În ultimele șase luni au fost realizate progrese importante în identificarea lacunelor în pregătirea pentru incidente de securitate de natură chimică, biologică, radiologică și nucleară, în special în ceea ce privește capacitatea de detecție pentru a contribui la prevenirea atacurilor chimice, biologice, radiologice și nucleare. La inițiativa Comisiei, un grup de experți naționali a efectuat o analiză a lacunelor în ceea ce privește echipamentele de detectare pentru diferite tipuri de scenarii legate de atacuri chimice, biologice, radiologice și nucleare. Raportul privind analiza lacunelor a fost comunicat statelor membre, permițându-le acestora să ia decizii în cunoștință de cauză cu privire la strategiile de detectare și să ia măsuri operaționale pentru a remedia lacunele identificate.

Această activitate a fost susținută prin exerciții de testare a nivelului de progres. Exercițiul paralel și coordonat din 2017 (PACE17) cu Organizația Tratatului Atlanticului de Nord a permis o testare detaliată a capacităților de reacție ale UE la criza hibridă pe scară largă. Fără precedent în ceea ce privește domeniul de aplicare, acest exercițiu a testat nu numai „protocolul UE de combatere a amenințărilor hibride" (*EU Playbook*), diferitele mecanisme de reacție ale UE și capacitatea acestora de a interacționa în mod eficient unele cu altele, ci și modul în care reacția UE la amenințările hibride a interacționat cu acțiunea Organizației Tratatului Atlanticului de Nord. Un exercițiu pentru 2018 este în faza de planificare, cu ambiția nu numai ca acesta să devină o practică anuală, ci și de a sprijini statele membre să își consolideze capacitățile de reacție în situații de criză hibridă.

Aceste măsuri concrete ilustrează modul în care cadrele de politică instituite de UE încep să dea roade: în ultimii doi ani s-au înregistrat o serie de cadre destinate să contribuie la orientarea și concentrarea activității UE.

Cadrul comun privind contracararea amenințărilor hibride – un răspuns al Uniunii Europene[12] din aprilie 2016 a încurajat o abordare la nivelul întregii administrații, cu 22 de domenii de acțiune, pentru a contribui la contracararea **amenințărilor hibride** și la promovarea rezilienței UE și a statelor membre, precum și a partenerilor internaționali. Majoritatea acțiunilor definite în cadrul comun pun accent pe îmbunătățirea conștientizării situației și pe consolidarea rezilienței, cu o mai bună capacitate de reacție. Acestea variază de la îmbunătățirea capacităților UE de analiză a informațiilor la consolidarea protecției infrastructurilor critice și a securității cibernetice la lupta împotriva radicalizării și a extremismului violent. Amenințările cibernetice și atacurile cibernetice se află, de asemenea, în centrul cadrului comun. Al doilea raport privind progresele înregistrate cu privire la punerea în aplicare a cadrului comun, adoptat în paralel cu prezenta comunicare comună, demonstrează progresele concrete în ceea ce privește aceste acțiuni și confirmă consolidarea și aprofundarea eforturilor UE de a contracara amenințările hibride[13].

În ceea ce privește **securitatea cibernetică**, 9 mai 2018 a reprezentat un moment important, fiind termenul-limită pentru ca toate statele membre ale UE să transpună primul set de norme obligatorii din punct de vedere juridic la nivelul UE privind securitatea cibernetică, și anume Directiva privind securitatea rețelelor și a sistemelor informatice. Aceasta este o parte importantă din abordarea mai amplă stabilită în Comunicarea comună *„Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE"*[14] din septembrie 2017, conținând o serie de măsuri concrete pentru a stimula în mod semnificativ capacitățile și structurile de securitate cibernetică ale UE. Comunicarea s-a axat pe consolidarea rezilienței UE în fața atacurilor cibernetice și pe consolidarea capacității în materie de securitate cibernetică a UE; crearea unui răspuns eficace prevăzut

[13] Pentru primul raport de punere în aplicare (iulie 2017): JOIN(2017) 30 final.
[14] JOIN(2017) 450 final.

de dreptul penal; și consolidarea stabilității globale prin cooperare internațională. Aceasta a fost însoțită de o propunere de Lege privind securitatea cibernetică pentru consolidarea sprijinului acordat la nivelul UE[15] și a fost susținută de o serie de propuneri care trebuie continuate până la punerea în aplicare (a se vedea mai jos).

Dezinformarea are efecte nocive asupra democrațiilor noastre afectând capacitatea cetățenilor de a lua decizii în cunoștință de cauză și de a participa la procesul democratic. Internetul a crescut considerabil volumul și varietatea știrilor aflate la dispoziția cetățenilor. Cu toate acestea, noile tehnologii pot fi utilizate pentru a difuza dezinformare la o viteză și cu o amploare fără precedent, determinând cu precizie publicul-țintă pentru a semăna neîncredere și a crea tensiuni societale. *Comunicarea Comisiei privind combaterea dezinformării online: o abordare europeană*[16] a stabilit o abordare europeană pentru a răspunde la problema dezinformării solicitând diferitelor părți interesate, în special platformelor online, dar și societăților din sectorul mass-media, să ia măsuri. Aceste măsuri acoperă o gamă largă de domenii relevante, inclusiv o mai mare transparență; credibilitatea și responsabilitatea platformelor online; procese electorale mai sigure și mai reziliente; stimularea educației, inclusiv în domeniul mass-mediei; sprijinirea jurnalismului de calitate; și contracararea dezinformării prin comunicare strategică. Primele etape concrete includ un Cod de bune practici privind dezinformarea, care urmează să fie elaborat de un Forum multilateral privind dezinformarea, precum și o rețea de verificatori ai veridicității informațiilor care va fi instituită până în această vară. Prima reuniune a Forumului multilateral privind dezinformarea a avut loc la 29 mai 2018, convenindu-se asupra măsurilor necesare pentru a adopta codul în iulie 2018. Comisia va evalua, până la sfârșitul anului 2018, progresele realizate în abordarea acestei probleme și va decide dacă este necesară sau nu o intervenție suplimentară în domeniu. Activitățile prevăzute vor fi coerente și complementare cu cele ale grupului operativ East Stratcom.

În ceea ce privește riscurile **chimice, biologice, radiologice și nucleare**, *Planul de acțiune*[17] al Comisiei din octombrie 2017 a propus 23 de acțiuni concrete și măsuri vizând o mai bună protecție a cetățenilor și a infrastructurilor împotriva acestor amenințări, inclusiv prin intermediul unei cooperări mai strânse între UE și statele sale membre, precum și cu Organizația Tratatului Atlanticului de Nord. Ca parte a măsurilor din cadrul uniunii securității pentru a spori protecția și reziliența împotriva terorismului, planul a urmat o abordare preventivă bazată pe motivația că riscurile chimice, biologice, radiologice și nucleare aveau probabilitate scăzută de realizare, dar un impact major și de durată în cazul unui atac. În același timp, atacul de la Salisbury, precum și o preocupare sporită cu privire la interesul terorist și capacitatea de utilizare a materialelor CBRN atât în interiorul, cât și în afara UE[18] demonstrează că amenințarea reprezentată de substanțele chimice, biologice, radiologice și nucleare este reală. Aceasta întărește și mai mult necesitatea urgentă de a pune în aplicare pe deplin planul de acțiune. Planul urmează o abordare a tuturor riscurilor și se concentrează pe patru obiective: reducerea accesibilității materialelor chimice, biologice, radiologice și nucleare; asigurarea unei pregătiri și reacții mai solide la incidentele de securitate de natură chimică, biologică, radiologică și nucleară; consolidarea legăturilor interne-externe în domeniul securității chimice, biologice, radiologice și nucleare cu principalii parteneri regionali și internaționali ai UE; și consolidarea cunoștințelor despre riscurile chimice, biologice, radiologice și nucleare. Raportarea detaliată cu privire la progresele concrete înregistrate în punerea în aplicare a

---

15 COM (2017) 477, a se vedea mai jos.

16 COM (2018) 236 final.

17 COM(2017) 610 final.

18 Europol, Raport privind situația și tendințele terorismului (TE-SAT) 2017, p. 16, disponibil la adresa: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. A se vedea, de asemenea, declarația directorului general al OIAC: www.globaltimes.cn/content/1044644.shtml.

planului de acțiune este prevăzută în cel mai recent raport privind progresele înregistrate către o uniune a securității, adoptat în paralel cu prezenta comunicare comună.

În final, pentru a spori eficacitatea eforturilor de combatere a amenințărilor hibride și pentru a consolida mesajul de unitate între statele membre ale UE și aliații NATO, cooperarea împotriva amenințărilor hibride a fost definită drept un domeniu-cheie al **cooperării UE-NATO**, astfel cum s-a subliniat în *Declarația comună de la Varșovia* din iulie 2016[19]. Aproape o treime din toate propunerile comune de cooperare actuale se axează pe amenințări hibride[20]. Exercițiile și „Protocolul UE de combatere a amenințărilor hibride" (EU Playbook)[21] descrise mai sus sunt urmate printr-o mai strânsă cooperare în acest an.

3. INTENSIFICAREA RĂSPUNSULUI LA AMENINȚĂRILE ÎN EVOLUȚIE

3.1. Conștientizarea situației – capacitatea îmbunătățită de a detecta amenințările hibride

Eforturile de a contracara amenințările hibride și de a răspunde acestora trebuie să fie susținute de o capacitate de detectare timpurie a surselor și a activităților hibride rău intenționate, interne și externe, și de înțelegere a eventualelor conexiuni între evenimente adesea aparent fără legătură. În acest scop, este esențial să se utilizeze toate datele disponibile, inclusiv informații din surse deschise.

Celula de fuziune împotriva amenințărilor hibride instituită în cadrul Serviciului European de Acțiune Externă ca punct focal unic european pentru analiza amenințărilor hibride constituie un atu important, dar are nevoie de cunoștințele de specialitate necesare pentru a aborda întregul spectru al amenințărilor hibride, inclusiv în domeniul chimic, biologic, radiologic și nuclear, precum și contrainformații. Extinderea cunoștințelor de specialitate ar crește sprijinul pentru orice reacție viitoare a UE în situații de criză prin oferirea de informații civile și militare mai complete în aceste domenii specifice. Acest lucru ar putea fi susținut prin acțiunile statelor membre de a crește numărul de informații cu care serviciile lor naționale contribuie la celula de fuziune împotriva amenințărilor hibride și de a consolida și mai mult capacitatea rețelei de puncte de contact naționale stabilite pentru celula de fuziune împotriva amenințărilor hibride de a furniza și a prelucra informații critice din punct de vedere al timpului. Un alt pas ar fi ca statele membre să analizeze posibilitatea creșterii numărului de informații cu care serviciile lor naționale contribuie la Centrul de situații și de analiză a informațiilor al UE (INTCEN), pentru a permite o analiză mai aprofundată a potențialelor amenințări.

---

19 Declarația semnată de președintele Juncker, președintele Tusk și Secretarul General al NATO, dl. Stoltenberg constituie baza actuală pentru cooperarea UE-NATO.

20 15283/16 și 14802/17.

21 SWD(2016) 227 final.

Măsuri viitoare

- Înaltul Reprezentant va extinde celula de fuziune a UE împotriva amenințărilor hibride cu contrainformații specializate de natură chimică, biologică, radiologică și nucleară, precum și cu elemente analitice cibernetice. Statele membre sunt invitate să sporească numărul de informații cu care contribuie la celula de fuziune împotriva amenințărilor hibride pentru analiza amenințărilor hibride existente și emergente.

- Comisia, în coordonare cu Înaltul Reprezentant, va finaliza lucrările cu privire la indicatorii de vulnerabilitate pentru a permite statelor membre să evalueze mai bine potențialul amenințărilor hibride în diferite sectoare. Această activitate va sprijini, de asemenea, analiza tendințelor hibride efectuată de UE.

3.2. **Acțiuni consolidate împotriva amenințărilor chimice, biologice, radiologice și nucleare**

Planul de acțiune împotriva riscurilor de siguranță chimică, biologică, radiologică și nucleară din octombrie 2017 stabilește cadrul de acțiune în vederea consolidării pregătirii, a rezilienței și a coordonării la nivelul UE. Acțiunile prevăzute în acesta acoperă o gamă de măsuri destinate să sprijine statele membre prin punerea în comun a cunoștințelor de specialitate și consolidarea capacităților comune, schimbul de cunoștințe și de cele mai bune practici și intensificarea cooperării operaționale. Statele membre și Comisia trebuie să conlucreze pentru a pune în aplicare pe deplin planul de acțiune în regim de urgență. În plus, bazându-se pe progresele deja înregistrate în ceea ce privește analiza lacunelor privind capacitățile de detectare și în schimbul de cele mai bune practici în ceea ce privește nou-creatul Grup consultativ pentru securitate chimică, biologică, radiologică și nucleară, Uniunea ar trebui în prezent să ia măsuri suplimentare pentru a aborda amenințările în evoluție. Acest lucru este valabil în special pentru amenințările chimice. Urmând exemplul acțiunilor pentru restricționarea accesului la precursorii de explozivi[22], UE trebuie să adopte măsuri operaționale rapide pentru a controla mai bine accesul la materialele chimice cu grad ridicat de risc și pentru a optimiza capacitatea de a detecta astfel de materiale în etape cât mai timpurii posibil. De asemenea, statele membre ar trebui să aibă în vedere efectuarea de analize ale lacunelor și de exerciții de cartografiere suplimentare la nivelul UE, de exemplu privind reziliența chimică, biologică, radiologică și nucleară și abordările și mijloacele de decontaminare. Pregătirea și gestionarea consecințelor unui atac chimic, biologic, radiologic și nuclear necesită o cooperare și o coordonare consolidată între statele membre, inclusiv între autoritățile de protecție civilă. Mecanismul de protecție civilă al Uniunii poate îndeplini un rol esențial în acest proces, în scopul consolidării capacității colective de pregătire și de reacție a Europei.

De asemenea, cooperarea internațională este un element important în această activitate, iar UE se poate baza pe legăturile cu centrele de excelență regionale în domeniul CBRN, inclusiv prin căutarea de sinergii cu Organizația Tratatului Atlanticului de Nord și

[22] Ca parte a activităților în cadrul uniunii securității pentru închiderea spațiului în care operează teroriștii și infractorii, Comisia a luat măsuri ferme pentru a reduce accesul la precursorii de explozivi care pot fi utilizați impropriu pentru fabricarea de explozivi artizanali. În octombrie 2017, Comisia a prezentat o recomandare stabilind măsuri imediate de prevenire a utilizării improprii a precursorilor de explozivi, bazată pe normele existente [Recomandarea C(2017) 6950 final]. Pe această bază, Comisia a adoptat în aprilie 2018 o propunere pentru revizuirea și consolidarea actualului Regulament (UE) nr. 98/2013 privind comercializarea și utilizarea precursorilor de explozivi [COM(2018) 209 final].

programe de prevenire, pregătire și răspuns la dezastre naturale sau provocate de om pentru țările din sud și din est[23].

Măsuri viitoare

- UE ar trebui să analizeze măsuri care să susțină respectarea normelor și standardelor internaționale împotriva utilizării armelor chimice, inclusiv prin intermediul unui posibil regim specific de sancțiuni ale UE privind armele chimice.
- Pentru a avansa planul de acțiune în domeniul chimic, biologic, radiologic și nuclear, Comisia va colabora cu statele membre pentru a finaliza până la sfârșitul anului 2018 următoarele etape:
  - elaborarea unei liste de substanțe chimice care constituie o amenințare specială, ca bază pentru acțiunile operaționale pentru a reduce accesibilitatea acestora;
  - instituirea unui dialog cu actori privați din lanțul de aprovizionare pentru a colabora în vederea abordării amenințărilor în evoluție cauzate de substanțe chimice care pot fi utilizate ca precursori;
  - accelerarea unei revizuiri a scenariilor de amenințare și a unei analize a metodelor de detectare existente pentru a îmbunătăți detectarea amenințărilor chimice, cu scopul de a dezvolta orientări operaționale pentru ca statele membre să își intensifice capacitățile de detectare.
- Statele membre ar trebui să stabilească inventare privind stocurile de contramăsuri medicale esențiale, laboratoare, tratamente și alte capacități. Comisia va colabora cu statele membre pentru a cartografia în mod regulat disponibilitatea acestor stocuri în întreaga UE pentru a spori accesibilitatea și mobilizarea rapidă a acestora în cazul unor atacuri.

3.3. **Comunicarea strategică – diseminarea coerentă a informațiilor**

O provocare importantă în ceea ce privește amenințările hibride constă în a sensibiliza și a educa publicul larg să discearnă informațiile de dezinformare. Bazându-se pe experiența grupului operativ East Stratcom, celula de fuziune a UE împotriva amenințărilor hibride și Centrul European de Excelență pentru Contracararea Amenințărilor Hibride, precum și pe alte eforturi depuse de Comisie[24], Comisia și Înaltul Reprezentant vor dezvolta în continuare și vor profesionaliza capabilitățile de comunicare strategică ale UE, prin asigurarea interacțiunii sistematice și a coerenței între structurile existente. Aceasta va fi extinsă la alte instituții ale UE și la alte state membre, inclusiv prin utilizarea anunțatei platforme online securizate privind dezinformarea.

O mai bună coordonare și cooperare în privința comunicării strategice în cadrul instituțiilor UE, cu statele membre și cu partenerii și organizațiile internaționale va fi esențială și necesită pregătire și practică înainte de a reacționa la crizele în timp real.

---

[23] În vecinătatea estică și sudică, în cadrul programelor regionale de prevenire, pregătire și răspuns la dezastre naturale și provocate de om sunt organizate cursuri de formare și exerciții în materie de protecție civilă.

[24] De exemplu, reprezentanțele Comisiei sunt active, de asemenea, în domeniul verificării factuale și al combaterii ideilor preconcepute. Mai multe reprezentanțe au elaborat instrumente adaptate la nivel local, cum ar fi *Les Décodeurs de l'Europe* în Franța, UE Vero Falso în Italia, un concurs public UE de benzi desenate Mythbusters în Austria, o serie de benzi desenate similare în România și Euromiturile de la A la Z ale reprezentanței Regatului Unit. Mai multe astfel de proiecte sunt în curs de elaborare.

Perioadele electorale s-au dovedit a fi o țintă deosebit de sensibilă și strategică pentru atacurile facilitate de tehnologiile informatice și eludarea online a garanțiilor și regulilor convenționale („offline”) precum perioadele tacite, normele de finanțare transparente și tratamentul egal al candidaților. Acestea au inclus atacurile împotriva infrastructurilor electorale și sistemelor informatice de campanie, precum și campanii online de dezinformare în masă motivate politic și atacuri cibernetice comise de țări terțe cu scopul de a discredita și a anula legitimitatea alegerilor democratice. Mai multe direcții de lucru sunt extinse la nivelul UE pentru a sensibiliza statele membre în pregătirea și răspunsul la aceste amenințări în evoluție. În cadrul Consiliului, autoritățile cu atribuții de securitate cibernetică ale statelor membre[25] vor emite orientări voluntare și vor defini cele mai bune practici comune pentru a aborda securitatea informatică a tehnologiei electorale de-a lungul ciclului electoral. Acestea includ sistemele de informații și soluțiile TIC utilizate pentru înregistrarea alegătorilor și a candidaților, pentru colectarea și numărarea voturilor și transmiterea rezultatelor, precum și sistemele auxiliare direct legate de legitimitatea rezultatelor alegerilor.

De asemenea, este necesar să se asigure informații rapide, fiabile și coerente destinate publicului larg în cazul atacurilor hibride. Orice incident chimic, biologic, radiologic și nuclear sau eveniment cu impact similar generează proteste publice, cetățenii solicitând răspunsuri rapide. Comunicarea strategică joacă un rol-cheie, inclusiv între organizațiile internaționale care își pot aplica separat planurile de intervenție.

Măsuri viitoare

- Serviciul European de Acțiune Externă și Comisia vor colabora în cadrul competențelor lor respective pentru a stabili o cooperare mai structurată privind comunicările strategice de abordare a dezinformării emanate din interiorul și din afara UE și pentru a descuraja dezinformarea ostilă și interferența hibridă din partea guvernelor străine.

- Comisia va organiza în toamnă evenimente la nivel înalt cu statele membre și părțile interesate relevante, inclusiv Colocviul privind drepturile fundamentale dedicat democrației, pentru a promova cele mai bune practici și orientări privind modul de a preveni, a atenua și a răspunde la amenințările facilitate de tehnologiile informatice și de dezinformare la adresa alegerilor.

- Înaltul Reprezentant și Comisia Europeană vor analiza modalități, în ceea ce privește instrumentele și resursele, de a sprijini mai bine activitatea desfășurată de cele trei grupuri operative Stratcom în scopul de a garanta că eforturile UE sunt suficient de extinse pentru a aborda complexitatea campaniilor de dezinformare desfășurate de entități ostile.

3.4. **Consolidarea rezilienței și a prevenirii în sectorul securității cibernetice**

Securitatea cibernetică este esențială atât pentru prosperitatea, cât și pentru securitatea noastră. Întrucât viața noastră de zi cu zi și economiile noastre depind tot mai mult de tehnologiile digitale, am devenit din ce în ce mai expuși.

Securitatea cibernetică efectivă în UE în ziua de astăzi este afectată de investiții insuficiente și de o coordonare insuficientă. UE încearcă în prezent să abordeze acest

[25] Sub auspiciile grupului de cooperare instituit în temeiul Directivei privind securitatea rețelelor și a sistemelor informatice.

aspect prin consolidarea capacităților prin măsuri de sprijin, o mai bună coordonare și noi structuri pentru a realiza progrese tehnologice și implementarea în domeniul securității cibernetice[26]. Directiva privind securitatea rețelelor și a sistemelor informatice[27] a stabilit un nivel minim de securitate a rețelelor și a sistemelor informatice în Uniune. Punerea sa deplină în aplicare de către toate statele membre este esențială pentru creșterea rezilienței cibernetice: acesta este un prim pas important. Regulamentul general privind protecția datelor introduce obligația de a notifica încălcarea securității datelor cu caracter personal către autoritatea de supraveghere competentă. Alte măsuri-cheie includ consolidarea și modernizarea Agenției europene de securitate cibernetică și un cadru de certificare la nivelul UE pentru produsele și serviciile TIC[28] pentru a consolida încrederea consumatorilor. Activitatea de sprijinire a rețelei de centre de competență ale statelor membre pentru a stimula dezvoltarea și implementarea de soluții de securitate cibernetică și pentru a completa eforturile de consolidare a capacității în domeniu la nivelul UE și la nivel național este, de asemenea, în curs de desfășurare. Aceasta se va baza pe activitatea programului Europa digitală, prezentat de Comisie la 6 iunie[29], care oferă o nouă prioritate pentru investițiile UE în securitatea cibernetică.

În același timp, o Recomandare privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare („Planul de acțiune”)[30] definește modul în care ar trebui să funcționeze cooperarea între statele membre și diferiții actori ai UE atunci când răspund la un atac cibernetic transfrontalier de mare amploare. Planul a subliniat rolul esențial al conștientizării situației pentru o coordonare eficace la nivelurile tehnic, operațional și strategic/politic. Grupul de cooperare instituit în temeiul Directivei privind securitatea rețelelor și a sistemelor informatice face, de asemenea, eforturi pentru a îmbunătăți schimbul și diseminarea de informații între părțile relevante, dezvoltând o taxonomie comună pentru descrierea unui incident. Această abordare va fi testată în cadrul viitoarelor exerciții. Analiza strategică a amenințărilor cibernetice actuale și emergente, pe baza contribuțiilor serviciilor de informații ale statelor membre, este furnizată de celula de fuziune împotriva amenințărilor hibride.

Cadrul pentru un răspuns diplomatic comun al UE la activități informatice răuvoitoare („setul de instrumente pentru diplomația cibernetică”) a constituit un important pas înainte din punct de vedere operațional, stabilind măsuri în cadrul politicii externe și de securitate comună, inclusiv măsuri restrictive care pot fi utilizate pentru a consolida răspunsul UE la activități care aduc atingere intereselor sale politice, economice și de securitate. Cu cât acest cadru este utilizat mai pe deplin de către statele membre, cu atât acesta va acționa ca un factor de descurajare eficace. În luna aprilie, Consiliul Afaceri Externe a adoptat concluzii privind activitățile cibernetice răuvoitoare care au condamnat în mod ferm utilizarea rău intenționată a tehnologiilor informației și comunicațiilor, inclusiv în atacurile Wannacry și NotPetya, care au provocat daune și pierderi economice semnificative în UE și în afara acesteia.

UE și statele sale membre trebuie să își îmbunătățească capacitatea de a atribui atacurile cibernetice, nu în ultimul rând prin intensificarea schimbului de informații. Atribuirea ar descuraja potențialii agresori și ar spori șansele ca persoanele responsabile să fie trase la răspundere în mod corespunzător. Creșterea prevenirii este un obiectiv-cheie al abordării

---

[26] În cadrul consolidării inovării în regiunile Europei, în decembrie 2017 a fost lansată o nouă acțiune-pilot interregională care reunește regiunile UE pentru a intensifica activitățile în domeniul securității informatice.

[27] Directiva 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.

[28] COM (2017) 477.

[29] Propunere de regulament de instituire a programului Europa digitală pentru perioada 2021-2027, COM(2018) 434.

[30] C(2017) 6100.

strategice a Comisiei în vederea consolidării securității cibernetice. Recentele propuneri ale Comisiei care vizează îmbunătățirea colectării transfrontaliere a probelor electronice în cadrul procedurilor penale ar spori, de asemenea, considerabil capacitatea autorităților de aplicare a legii de a ancheta și a urmări în justiție criminalitatea informatică.

Reziliența cibernetică necesită o abordare amplă și colectivă. Aceasta impune structuri mai solide și eficace pentru a promova securitatea cibernetică și pentru a reacționa la atacuri informatice în statele membre, precum și în instituțiile, agențiile, delegațiile, misiunile și operațiunile proprii ale UE: lipsa unei rețele comune de comunicații securizate între instituțiile europene reprezintă o deficiență importantă. Ar trebui să se sporească gradul de sensibilizare cu privire la aspectele de securitate informatică în instituțiile UE și în rândul personalului acestora printr-o îmbunătățire a culturii securității și printr-o instruire intensificată.

Măsuri viitoare

- Parlamentul European și Consiliul ar trebui să își accelereze lucrările pentru a încheia negocierile cu privire la propunerile în materie de securitate cibernetică prin intermediul unui acord până la sfârșitul acestui an și să convină asupra propunerii legislative privind colectarea de probe electronice.

- Comisia și Înaltul Reprezentant vor colabora îndeaproape cu statele membre pentru a promova aspectele cibernetice ale mecanismelor de gestionare a crizelor și de reacție la nivelul UE. Statele membre sunt invitate să își continue activitățile cu privire la atribuirea atacurilor cibernetice și utilizarea practică a setului de instrumente pentru diplomația cibernetică pentru a accelera răspunsul politic la atacurile cibernetice.

- Ca răspuns la necesitatea de a intensifica capacitățile de apărare cibernetică, se înființează o platformă specifică de formare și educație pentru a contribui la coordonarea posibilităților de formare în domeniul apărării cibernetice oferite de statele membre. Vor fi căutate sinergii cu eforturile similare depuse de Organizația Tratatului Atlanticului de Nord.

3.5. **Consolidarea rezilienței față de activitățile ostile de informații**

Contracararea activităților ostile de informații necesită, în primul rând, o coordonare sporită între statele membre, în conformitate cu normele și procedurile UE și naționale relevante. Cu toate acestea, este imperativă creșterea capacităților instituțiilor UE de a contracara amenințarea crescândă pe care o constituie o astfel de activitate care vizează în mod special instituțiile și crearea unei culturi de conștientizare a aspectelor de securitate, susținută de o mai bună formare și securitate fizică. Instituțiile ar putea, de asemenea, să colaboreze cu statele membre pentru a construi un sistem de acreditare al UE mai solid. Un astfel de sistem ar trebui să se bazeze pe raportarea proactivă, permițând o mai bună conștientizare în rândul statelor membre și al instituțiilor cu privire la posibile entități ostile, mai ales cele deja identificate de către statele membre.

Coordonarea dintre statele membre și între statele membre și alte organizații internaționale relevante, cum ar fi Organizația Tratatului Atlanticului de Nord în special, ar putea contribui la canalizarea contrainformațiilor împotriva unor activități ostile în UE. Un exemplu de domeniu care ar beneficia de o coordonare consolidată între statele membre

este examinarea investițiilor, pe baza unui regulament[31] propus de Comisie în septembrie 2017 pentru examinarea investițiilor străine directe de către statele membre din motive de securitate sau de ordine publică. O coordonare sporită între statele membre ar fi la fel de importantă pentru monitorizarea tranzacțiilor financiare, întrucât serviciile de informații ostile își finanțează din ce în ce mai mult măsurile active împotriva UE prin mecanisme de finanțare complexe.

Măsuri viitoare

- Serviciul European de Acțiune Externă și Comisia Europeană vor pune în aplicare măsuri practice îmbunătățite pentru a susține și a dezvolta capacitatea UE de a interacționa cu statele membre în scopul de a combate activitățile ostile de informații direcționate în mod specific asupra instituțiilor.
- Celula de fuziune împotriva amenințărilor hibride consolidată va fi completată cu expertiza serviciilor de contrainformații pentru a furniza analize și informări detaliate cu privire la natura activităților ostile de informații probabile împotriva persoanelor și instituțiilor.
- Parlamentul European și Consiliul ar trebui să accelereze eforturile în vederea încheierii negocierilor privind propunerea de examinare a investițiilor până la sfârșitul anului.

4. CONCLUZIE

Amenințările hibride și amenințările chimice, biologice, radiologice și nucleare fac parte dintre preocupările majore ale UE. Incidentul din martie din Regatul Unit a evidențiat spectrul larg al războiului hibrid și necesitatea deosebită de dezvoltare a rezilienței față de amenințările chimice, biologice, radiologice și nucleare.

Comisia și Înaltul Reprezentant au adoptat și au propus o serie de inițiative pentru a aborda provocările reprezentate de amenințările hibride. De asemenea, Comisia accelerează punerea în aplicare a Planului de acțiune din 2017 privind îmbunătățirea nivelului de pregătire împotriva riscurilor de siguranță chimică, biologică, radiologică și nucleară.

Prezenta comunicare comună are scopul de a informa Consiliul European cu privire la activitățile deja în curs și de a identifica domenii în care acțiunile ar trebui intensificate pentru a aprofunda și a consolida contribuția esențială a UE la abordarea acestor amenințări. În prezent, depinde de statele membre, de Comisie și de Înaltul Reprezentant să asigure acțiuni ulterioare rapide.

[31] Propunere de regulament al Parlamentului European și al Consiliului de stabilire a unui cadru pentru examinarea investițiilor străine directe în Uniunea Europeană, COM(2017) 487.