Consiliul
Uniunii Europene

Bruxelles, 27 mai 2022
(OR. en)

9563/22

JAI 761	**DROIPEN 69**
COSI 149	**COPEN 210**
ENFOPOL 298	**FREMP 110**
ENFOCUSTOM 89	**JAIEX 61**
IXIM 145	**CFSP/PESC 705**
CT 99	**COPS 238**
CRIMORG 81	**HYBRID 49**
FRONT 218	**DISINFO 47**
ASIM 47	**TELECOM 248**
VISA 87	**DIGIT 108**
CYBER 191	**COMPET 408**
DATAPROTECT 175	**RECH 307**
CATS 30	

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	25 mai 2022
Destinatar:	Secretariatul General al Consiliului
Nr. doc. Csie:	COM(2022) 252 final
Subiect:	COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU referitoare la cel de al patrulea raport privind punerea în aplicare a Strategiei UE privind o uniune a securității

În anexă, se pune la dispoziția delegațiilor documentul COM(2022) 252 final.

Anexă: COM(2022) 252 final

COMISIA
EUROPEANĂ

Bruxelles, 25.5.2022
COM(2022) 252 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

referitoare la cel de al patrulea raport privind punerea în aplicare a Strategiei UE privind o uniune a securității

I. INTRODUCERE

Războiul rus de agresiune împotriva Ucrainei domină actuala agendă de securitate a UE. Războiul nu numai că amenință Ucraina, ci urmărește să aducă prejudicii stabilității și securității mondiale. În interiorul UE, acesta implică o serie de riscuri pentru securitatea cetățenilor. Există noi incertitudini cu privire la aprovizionarea cu energie și cu alte materii prime, iar infrastructura critică poate fi ținta atacurilor cibernetice. Siguranța și securitatea interne ale UE sunt puse în pericol de potențiale atacuri sau accidente cauzate de agenți chimici, biologici sau radiologici din zona de război. Vulnerabilitățile a milioane de persoane care au fugit de război pot fi exploatate rapid de criminalitatea organizată, prin traficul de femei și copii, care sunt deosebit de expuși riscurilor.

În fața acestor noi și potențiale amenințări, UE a rămas fermă și unită. Deși, până acum, impactul războiului a rămas în principal limitat la teritoriul Ucrainei, UE și-a intensificat *vigilența și coordonarea*, împreună cu monitorizarea sporită a situației amenințărilor, și depune eforturi pentru a consolida reziliența în vederea asigurării *pregătirii*.

În Declarația de la Versailles din 10-11 martie 2022[1], liderii europeni au subliniat necesitatea de a ne pregăti pentru provocările care apar rapid, inclusiv „protejându-ne împotriva războiului hibrid din ce în ce mai intens, consolidându-ne reziliența cibernetică, protejându-ne infrastructura – în special infrastructura critică – și combătând dezinformarea".

Cadrul privind o uniune a securității este esențial pentru asigurarea securității în întreaga UE. Cele patru priorități strategice stabilite în Strategia UE privind o uniune a securității[2] rămân direct relevante în ceea ce privește această sarcină în contextul geopolitic actual: (i) un mediu de securitate adaptat exigențelor viitorului; (ii) combaterea amenințărilor în continuă evoluție; (iii) protejarea europenilor împotriva terorismului și a criminalității organizate și (iv) un ecosistem european solid în materie de securitate. Războiul a subliniat necesitatea ca UE și statele sale membre să utilizeze pe deplin instrumentele legislative și de politică deja disponibile în cadrul Strategiei UE privind o uniune a securității, care stau la baza sprijinului coordonat acordat de UE statelor membre în ceea ce privește aspecte precum criminalitatea organizată și terorismul, securitatea cibernetică și amenințările hibride.

Agențiile europene din domeniul justiției și afacerilor interne și-au intensificat, de asemenea, eforturile ca răspuns la războiul din Ucraina, jucând un rol esențial în evaluarea amenințărilor și în sprijinirea răspunsului operațional[3]. Consolidarea continuă a practicii operaționale și a guvernanței în spațiul Schengen reprezintă un alt factor important.

Acest al patrulea raport intermediar privind uniunea securității se axează pe evoluțiile din ultimele luni de la începerea războiului rus de agresiune împotriva Ucrainei. Acesta oferă o imagine de ansamblu a acțiunilor întreprinse cu privire la toate componentele uniunii securității și ia în considerare nevoile de pregătire care decurg din potențialele amenințări la adresa securității generate de războiul din Ucraina. Progresele înregistrate cu privire la alte dosare privind uniunea securității se regăsesc în anexă.

---

1 https://www.consilium.europa.eu/media/54785/20220311-versailles-declaration-ro.pdf.
2 COM(2020) 605.
3 Declarația comună a agențiilor UE din domeniul justiției și afacerilor interne cu privire la Ucraina | Agenția Uniunii Europene pentru Azil (europa.eu).

II. SECURITATEA CIBERNETICĂ ȘI INFRASTRUCTURA CRITICĂ

De la izbucnirea războiului, actori privați și operațiuni infracționale au făcut public faptul că desfășoară activități cibernetice în sprijinul uneia sau alteia dintre părți. Hacktivism-ul[4] reprezintă o amenințare din cauza riscului de efecte de propagare în UE împotriva serviciilor critice, a riscului de atacuri din partea rețelelor oficiale sau a altor efecte neprevăzute de propagare. Deși, până acum, războiul s-a desfășurat în mare parte cu mijloace convenționale și cu efecte limitate de propagare, riscul de escaladare în acest domeniu este real.

Prin urmare, UE și-a intensificat coordonarea și pregătirea. Amenințările generate de război subliniază necesitatea de a construi o cultură a schimbului de informații și de expertiză între UE, statele membre și comunitățile de securitate cibernetică. Aceasta include consolidarea conștientizării integrate a situației, împărtășită de instituțiile, organele și agențiile UE și de statele membre, în special în ceea ce privește infrastructura critică de care depinde buna funcționare a pieței interne.

Atribuirea atacurilor cibernetice împotriva Ucrainei

Atacurile cibernetice împotriva Ucrainei au început chiar înainte de agresiunea Rusiei și, în primele zile ale războiului[5], au urmărit compromiterea conturilor de utilizator ale personalului militar ucrainean și perturbarea serviciilor esențiale, inclusiv a controlului frontierelor și a telecomunicațiilor.

La 14 ianuarie 2022, înaltul reprezentant a făcut o declarație[6] în numele Uniunii Europene prin care a condamnat atacurile cibernetice împotriva Ucrainei și a reafirmat sprijinul fără echivoc al UE pentru Ucraina.

La 10 mai, Uniunea Europeană și statele sale membre, împreună cu partenerii internaționali, au condamnat cu fermitate[7] activitatea cibernetică răuvoitoare împotriva Ucrainei din 24 februarie, care a avut ca țintă rețeaua satelitară KA-SAT, deținută de Viasat, și au atribuit direct atacul Federației Ruse. Acest atac cibernetic a avut un impact semnificativ, cauzând întreruperi și perturbări generalizate ale comunicării între mai multe autorități publice, întreprinderi și utilizatori din Ucraina, precum și afectând mai multe state membre ale UE.

Vigilență și coordonare

[4] Un exemplu recent de hacktivism este utilizarea „protestware-ului” pentru a răspândi programe malware pe IP-uri rusești prin intermediul unui pachet popular cu sursă deschisă, ceea ce ar putea duce la riscuri în cadrul lanțului de aprovizionare și la pierderea încrederii în comunitatea de tip „open source”. Comisia a clarificat faptul că atacurile cibernetice împotriva Rusiei (până și cele bine intenționale) sunt ilegale.

[5] Raportul special al Microsoft: „An overview of Russia’s cyberattack activity in Ukraine” (O prezentare generală a activității Rusiei de atac cibernetic în Ucraina); „The hybrid war in Ukraine - Microsoft On the Issues” (Războiul hibrid din Ucraina – Microsoft pe această temă).

[6] https://www.consilium.europa.eu/ro/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/.

[7] Operațiunile cibernetice ale Rusiei împotriva Ucrainei: Declarația Înaltului Reprezentant în numele Uniunii Europene – Consilium (europa.eu).

De la izbucnirea războiului rus de agresiune împotriva Ucrainei, monitorizarea situației securității cibernetice în statele membre și în instituțiile UE s-a intensificat. ENISA, Agenția Uniunii Europene pentru Securitate Cibernetică, Centrul european de combatere a criminalității informatice al Europol, CERT-UE - Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE - și Centrul de situații și de analiză a informațiilor al UE (INTCEN UE) au contribuit la conștientizarea comună a situației de către UE, inclusiv prin asigurarea monitorizării periodice a activităților cibernetice suspecte, inclusiv în sectoare specifice, cum ar fi energia, transporturile și aviația, și au oferit evaluări pentru a orienta acțiunile preventive.

De asemenea, s-au intensificat coordonarea și schimbul de informații cu rețelele de securitate cibernetică, cum ar fi Rețeaua organizațiilor de legătură în materie de crize cibernetice (CyCLONe), care include agenții naționale de securitate cibernetică, Comisia și ENISA. Pentru a reflecta această abordare la nivel intern în instituțiile UE, un mecanism de coordonare, Grupul operativ în materie de crize cibernetice, permite schimbul de informații între toate serviciile, organele și agențiile relevante, inclusiv ENISA, Centrul european de combatere a criminalității informatice al Europol și CERT UE. Sunt necesare eforturi constante pentru a asigura canale de comunicare între nivelul politic, cel operațional și cel tehnic, precum și pentru a consolida cooperarea cu Rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT).

Europol a activat, de asemenea, Protocolul UE privind răspunsul în caz de urgență al autorităților de aplicare a legii, care permite consolidarea monitorizării amenințărilor cibernetice și a schimbului de informații între o multitudine de părți interesate, pentru a avea o imagine cuprinzătoare a informațiilor cibernetice.

Pe lângă amenințările cibernetice, statele membre, SEAE și serviciile Comisiei au sporit vigilența în ceea ce privește expunerea infrastructurilor critice la amenințări fizice, altele decât cele cibernetice. Infrastructurile critice și entitățile care le exploatează pot fi expuse unor riscuri fizice, cum ar fi sabotajul de către un stat sau de către actori sponsorizați de stat, ca parte a unor posibile măsuri de retorsiune împotriva UE.

Pregătirea

Pregătirea în domeniul securității cibernetice și al securității infrastructurii critice este mai importantă ca niciodată, având în vedere expunerea sporită a Europei la o acumulare de amenințări generate de război. Eforturile de intensificare a pregătirii au inclus o serie de acțiuni directe, inclusiv unele care erau deja prevăzute înainte de agresiunea Rusiei împotriva Ucrainei. Printre acestea se numără exerciții, orientări, măsuri legislative, creșterea rezilienței în sectoarele critice și colaborarea cu partenerii.

Președinția franceză a Consiliului Uniunii Europene, împreună cu Serviciul European de Acțiune Externă (SEAE) și Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), a organizat un exercițiu bazat pe scenarii la începutul anului 2022, denumit CyCLES UE (Exercițiul de corelare a crizelor cibernetice privind solidaritatea), cu scopul de a crește gradul de conștientizare la nivel politic și de a consolida cooperarea între nivelul operațional și cel politic în cazul unui atac cibernetic de mare amploare.

În februarie, ENISA și CERT-UE au publicat **orientări** cu privire la modalitățile de creștere a rezilienței și a gradului de pregătire în UE[8]. Acestea încurajează toate organizațiile din sectorul public și privat din UE să adopte un set minim de bune practici în materie de securitate cibernetică pentru a îmbunătăți substanțial cultura securității cibernetice. În martie, CERT-UE a publicat orientări tehnice de monitorizare, cu sprijinul ENISA[9], precum și orientări privind securitatea pentru consolidarea configurării aplicației Signal[10], incluzând o serie de recomandări practice adresate organizațiilor în vederea îmbunătățirii posturii lor de securitate cibernetică.

Inițiative legislative

Situația actuală subliniază necesitatea urgentă **de a pune în aplicare legislația existentă** și de a accelera **adoptarea inițiativelor în curs**.

Comisia sprijină statele membre în ceea ce privește punerea în aplicare a **Directivei NIS**[11], care prevede ca statele membre să fie echipate în mod corespunzător, de exemplu, să dispună de o echipă de intervenție în caz de incidente de securitate informatică (CSIRT) și să desemneze autoritățile competente. Aceasta asigură baza pentru o cooperare eficace între statele membre. Acordul politic la care au ajuns colegiuitorii cu privire la **Directiva NIS2**[12] reprezintă un progres suplimentar în ceea ce privește asigurarea unui cadru solid de pregătire la nivelul UE.

NIS2 – Consolidarea în continuare a gradului de pregătire

- Noua Directivă privind rețelele și sistemele informatice va aborda deficiențele Directivei NIS anterioare, pentru a o adapta la nevoile actuale și la exigențele viitorului. Aceasta stabilește norme minime pentru un cadru de reglementare și mecanisme de cooperare eficace între autoritățile relevante din fiecare stat membru.
- Aceasta extinde domeniul de aplicare al normelor, adăugând noi sectoare esențiale pentru economie și societate (de exemplu, sectorul farmaceutic și cel al dispozitivelor medicale sau sectorul producției de alimente). Toate entitățile mijlocii și mari care își desfășoară activitatea în sectoarele respective sau prestează servicii reglementate de directivă vor intra în domeniul său de aplicare. Entitățile administrației publice din cadrul administrațiilor centrale (cu excepția sistemului judiciar, a parlamentelor și a băncilor centrale) și de la nivel regional sunt, de asemenea, incluse în domeniul de aplicare. În plus, statele membre pot decide ca directiva să se aplice entităților de la nivel local.
- Directiva NIS2 va stabili nivelul de referință pentru măsurile de gestionare a riscurilor în materie de securitate cibernetică și va institui în mod oficial Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (UE – CyCLONe), care va

[8] „Boosting your Organisation's Cyber Resilience – Joint Publication” (Îmbunătățirea rezilienței cibernetice a organizației dumneavoastră – Publicație comună), 14.2.2022.

[9] „Security Guidance 2002-01 - Cybersecurity mitigation measures against critical threats” (Orientările privind securitatea 22-001 – Măsuri de atenuare a amenințărilor critice la adresa securității cibernetice).

[10] „CERT-EU Security Guidance 22-002 - Hardening Signal” (Orientările CERT-EU privind securitatea 22-002 – Consolidarea securității aplicației Signal).

[11] 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.

[12] COM(2020) 823.

sprijini gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare.

- Propunerea introduce, de asemenea, dispoziții mai precise privind procesul de raportare a incidentelor, conținutul rapoartelor și termenele și prevede căi de atac și sancțiuni pentru a asigura respectarea legii.
- Statele membre vor avea la dispoziție 21 de luni de la intrarea în vigoare a directivei pentru a integra dispozițiile acesteia în legislația națională.

Progresele înregistrate în ceea ce privește Directiva NIS2 ar trebui să fie urmate cât mai curând posibil de finalizarea negocierilor referitoare la propunerea de **Directivă privind reziliența entităților critice**[13] („Directiva CER”), care, odată adoptată și pusă în aplicare, ar trebui să sporească reziliența entităților critice la o serie de amenințări, inclusiv atacuri teroriste, amenințări din interior sau sabotaj. De asemenea, este esențial ca nivelul de ambiție al Directivei privind reziliența entităților critice să corespundă celui din propunerea Comisiei și să se mențină coerența cu compromisul politic la care s-a ajuns cu privire la NIS2. Împreună, aceste măsuri vor stimula reziliența și pregătirea prin instituirea unui sistem mai coerent și mai robust, inclusiv prin intermediul planurilor naționale de răspuns la incidente și crize. Acestea au făcut parte, de asemenea, din recomandarea Comisiei de anul trecut[14] de creare a **unității cibernetice comune**, care stabilește modul în care diferiții actori ai ecosistemului de securitate cibernetică (diplomația, poliția, civilii și, după caz, apărarea) urmează să coopereze la nivel operațional. Situația actuală a amenințărilor subliniază valoarea unei astfel de cooperări eficiente între actorii-cheie.

Comisia continuă să monitorizeze punerea în aplicare a setului de instrumente privind securitatea cibernetică a rețelelor **5G**[15]. În acest context, la 11 mai, Grupul de cooperare NIS a adoptat un raport privind securitatea OpenRAN[16]. De asemenea, Comisia colaborează în continuare cu statele membre pentru ca Centrul european de competențe în materie de securitate cibernetică să devină pe deplin operațional.

La 22 martie 2022, Comisia a propus **noi norme pentru a stabili măsuri comune de securitate cibernetică și a informațiilor pentru toate instituțiile, organele și agențiile UE (EUIBA)**. Aceste norme vor consolida reziliența și capacitatea administrației UE de a răspunde la amenințările și incidentele cibernetice. Prin plasarea acestor activități într-un cadru comun, cooperarea interinstituțională va fi consolidată, iar expunerea la riscuri va fi redusă la minimum. Propunerea de **regulament privind securitatea cibernetică pentru instituțiile, organele și agențiile UE**[17] va consolida mandatul CERT-UE și va conduce la crearea unui nou consiliu interinstituțional pentru securitate cibernetică, va spori capacitățile în materie de securitate cibernetică și va stimula evaluări periodice ale maturității și o mai bună igienă cibernetică. **Regulamentul propus privind securitatea informațiilor**[18] va crea un set minim de norme și standarde de securitate a informațiilor pentru gestionarea și

[13] COM(2020) 829.
[14] Recomandarea privind înființarea unei unități cibernetice comune | Conturarea viitorului digital al Europei (europa.eu).
[15] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
[16] Grupul de cooperare NIS, „Report on the cybersecurity of Open RAN” (Raport privind securitatea cibernetică a Open RAN), 11 mai 2022.
[17] COM(2022) 122.
[18] COM(2022) 119.

schimbul securizat de informații ale tuturor instituțiilor, organelor, oficiilor și agențiilor UE, pentru a asigura o protecție sporită și coerentă împotriva amenințărilor în continuă evoluție la adresa informațiilor lor. Comisia invită Parlamentul European și Consiliul să adopte rapid aceste măsuri.

Comisia a finalizat consultarea publică privind măsurile de îmbunătățire a **rezilienței cibernetice** a produselor digitale și pregătește o propunere care urmează să fie publicată în această toamnă[19]. Aceasta va aborda vulnerabilitățile produselor digitale și ale serviciilor auxiliare care – deși creează oportunități pentru economiile și societățile din UE – determină și noi provocări, având în vedere că, cu cât totul este mai conectat, cu atât este mai ușor ca un incident de securitate cibernetică să afecteze un întreg sistem și, astfel, să perturbe activitățile economice și sociale.

La 9 martie 2022, miniștrii UE responsabili cu telecomunicațiile au adoptat în unanimitate Apelul de la Nevers de consolidare a capacităților UE în materie de securitate cibernetică, care include „punerea în aplicare a unui nou fond de răspuns în situații de urgență pentru securitatea cibernetică, care urmează să fie instituit de Comisie”[20]. Comisia analizează utilizarea optimă a fondurilor existente pentru a sprijini acțiunile preventive și de răspuns.

Sectoare critice

Securitatea aprovizionării cu **energie** a UE este esențială pentru bunăstarea cetățenilor și pentru buna funcționare a economiilor noastre, iar situația actuală a evidențiat necesitatea unor norme clare privind securitatea cibernetică în acest sector. Comisia lucrează la un cod de rețea privind securitatea cibernetică pentru fluxurile transfrontaliere de energie electrică, astfel cum se prevede în Regulamentul privind piața internă de energie electrică[21], pentru a prevedea norme privind evaluările riscurilor, cerințele minime comune, planificarea, monitorizarea, raportarea și gestionarea situațiilor de criză. De la izbucnirea războiului de agresiune al Rusiei împotriva Ucrainei, obiectivele avute în vedere pentru codul de rețea privind securitatea cibernetică sunt și mai relevante. Comisia a lansat, de asemenea, o cooperare structurală între ENISA, ENTSO-E[22], ENTSOG[23] și Comunitatea Energiei în ceea ce privește monitorizarea periodică a situației securității cibernetice în sectorul energetic.

UE a depus eforturi pentru a proteja securitatea partenerilor fără a crea noi riscuri pentru ea însăși. Sincronizarea de urgență a rețelelor electrice ale Ucrainei și Moldovei cu rețeaua Europei continentale a avut loc în martie 2022, după adoptarea măsurilor de atenuare a riscurilor, în special în ceea ce privește securitatea cibernetică.

Războiul și sancțiunile au creat, de asemenea, numeroase provocări pentru **transportul** european, de la riscuri la adresa siguranței aviației civile și a șoferilor de camioane din UE

[19] Actul privind reziliența cibernetică – noi cerințe în materie de securitate cibernetică pentru produsele digitale și serviciile auxiliare (europa.eu).

[20] 08/03/2022 - Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique - Presse - Ministère des Finances (economie.gouv.fr).

[21] Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului din 5 iunie 2019 privind piața internă de energie electrică (JO L 158, 14.6.2019, p. 54). În prezent, o propunere este în curs de revizuire de către Agenția pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei.

[22] Rețeaua europeană a operatorilor de sisteme de transport de energie electrică.

[23] Rețeaua europeană a operatorilor de transport și de sistem de gaze naturale.

blocați în zonele de conflict până la distrugerea infrastructurii de transport ucrainene, întreruperea lanțurilor de aprovizionare și amenințarea securității alimentare mondiale. Agenția Uniunii Europene pentru Siguranța Aviației, în strânsă cooperare cu Comisia și cu Eurocontrol, Organizația Europeană pentru Siguranța Navigației Aeriene, a recomandat operatorilor, încă de la începutul războiului, să nu opereze în spațiul aerian al Ucrainei și să evite utilizarea spațiului aerian pe o rază de 100 de mile marine de frontierele cu Ucraina, Belarus și Rusia.

De asemenea, Comisia a depus eforturi pentru a consolida gradul de pregătire și reziliența sectorului transporturilor din UE. În special, un nou plan de urgență pentru transporturi[24], adoptat la 23 mai, include lecții învățate atât ca urmare a pandemiei de COVID-19, cât și a agresiunii militare a Rusiei împotriva Ucrainei. Acesta propune un set de 10 acțiuni care să ghideze UE și statele sale membre atunci când introduc măsuri de răspuns în situații de urgență, inclusiv asigurarea conectivității minime, consolidarea rezilienței la amenințările cibernetice și la cele hibride și consolidarea cooperării cu partenerii internaționali în ceea ce privește pregătirea și răspunsul în situații de criză. Planul subliniază, de asemenea, importanța testării periodice a rezilienței pentru diferite scenarii de criză, care să reunească agențiile relevante ale UE sau alți actori și să se bazeze pe procesele existente.

În temeiul cadrului de **securitate sanitară al UE**, schimbul de informații bazat pe sistemul de alertă precoce și răspuns rapid, inclusiv sprijinul pentru evacuările medicale din Ucraina, trebuie să fie protejat împotriva atacurilor cibernetice, prin urmare, securitatea sistemului este în curs de consolidare.

Cooperarea cu partenerii

UE colaborează în continuare cu partenerii săi internaționali pentru a preveni, a descuraja, a împiedica și a răspunde la comportamentele răuvoitoare din spațiul cibernetic. Războiul de agresiune al Rusiei împotriva Ucrainei a făcut cooperarea în acest domeniu mai importantă ca niciodată. În acest sens, SEAE a depus eforturi pentru a face schimb de informații privind conștientizarea situației și coordonarea răspunsului la activitățile cibernetice răuvoitoare care vizează Ucraina, precum și privind sprijinul acordat Ucrainei și altor țări din regiune, prin colaborarea sa cu partenerii, inclusiv SUA și NATO, pentru a asigura complementaritatea și a evita suprapunerile.

Cooperarea strânsă cu SUA s-a intensificat, de asemenea, în contextul Consiliului UE-SUA pentru comerț și tehnologie (CCT). Declarația comună[25] emisă în urma reuniunii ministeriale de la Paris din luna mai a subliniat rolul central al CCT pentru parteneriatul transatlantic reînnoit, care servește la coordonarea măsurilor comune ale UE și SUA în contextul agresiunii Rusiei împotriva Ucrainei. Ambele părți au convenit că o cooperare strânsă pentru promovarea rezilienței lanțurilor de aprovizionare este mai importantă ca niciodată. În plus, un grup operativ dedicat finanțării publice pentru servicii și infrastructură digitală sigură și rezilientă în țări terțe a fost înființat pentru a pregăti terenul pentru finanțarea publică comună de către SUA și UE a unor proiecte digitale în țări terțe, bazate pe un set de principii generale comune.

Busola strategică adoptată în martie 2022 (a se vedea secțiunea VII) va consolida și mai mult setul de instrumente al UE pentru diplomația cibernetică și va dezvolta politica de apărare

[24] COM(2022) 21.
[25] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_3108.

cibernetică a UE pentru a fi mai bine pregătită pentru atacurile cibernetice și pentru a răspunde mai bine la acestea, ca parte a unei strategii mai ample de consolidare a capacității UE de a acționa în situații de criză și de a-și apăra interesele.

Sprijin în materie de securitate cibernetică pentru Ucraina și țările învecinate

UE oferea deja sprijin pentru reziliența cibernetică a Ucrainei înainte de începerea războiului. Încă din iunie 2021, UE și Ucraina au organizat un prim dialog cibernetic, iar UE a oferit acestei țări sprijin pentru securitatea cibernetică și transformarea digitală rezilientă, prin intermediul programului EU4Digital pentru Ucraina, în valoare de 25 de milioane EUR. Un program de înfrățire în valoare de 1,5 milioane EUR este conceput să ajute instituțiile din domeniul securității cibernetice din Ucraina să se alinieze la standardele UE.

În urma izbucnirii războiului, UE promovează cooperarea dintre experții UE și cei ucraineni în domeniul cibernetic și coordonează furnizarea de asistență tehnică, echipamente, software și servicii relevante pentru a consolida reziliența cibernetică și apărarea cibernetică a Ucrainei.

În plus, UE depune eforturi pentru a evalua un posibil sprijin pe termen mediu pentru Moldova, Georgia și Balcanii de Vest. O misiune comună de evaluare în Moldova cu privire la nevoile în materie de securitate cibernetică a fost efectuată în perioada 3-4 martie 2022 și a condus la adoptarea unei măsuri specifice de răspuns în situații de criză pentru a spori rapid securitatea cibernetică în țară. Un sprijin similar pentru răspuns rapid este în curs de pregătire pentru un număr restrâns de țări din Balcanii de Vest, considerate a fi deosebit de expuse riscului ca urmare a alinierii lor la sancțiunile impuse de UE. De asemenea, este în curs de evaluare o posibilă asistență suplimentară acordată Moldovei prin intermediul Instrumentului european pentru pace.

III. CRIMINALITATEA ORGANIZATĂ ȘI TERORISMUL

Războiul de agresiune al Rusiei împotriva Ucrainei a forțat milioane de persoane să își părăsească locuințele, determinând intensificarea considerabilă a traversării frontierelor externe ale UE. Până la 18 mai, aproape 6 milioane de persoane au sosit în UE din Ucraina și din Moldova, iar până în prezent 2,8 milioane s-au înregistrat pentru protecție temporară în UE. UE a încercat să ofere cea mai rapidă și mai flexibilă primire celor care fug din calea războiului, fără a compromite securitatea la frontiera externă a UE. UE a luat măsuri fără precedent pentru a le oferi celor care fug din calea războiului protecție temporară și se angajează să trateze toate sosirile noi fără discriminare. În același timp, riscurile potențiale care pot apărea din cauza numărului mare de persoane care se deplasează nu pot fi neglijate, iar UE, beneficiind de sprijin puternic din partea agențiilor UE relevante, rămâne vigilentă la noile evoluții în materie de criminalitate organizată și terorism.

Un spațiu Schengen puternic într-un moment în care amenințările sunt tot mai mari

Asigurarea unui nivel ridicat de securitate în spațiul **Schengen** și în cadrul UE nu a fost nicicând așa de importantă ca în contextul amenințărilor tot mai mari cauzate de războiul care se desfășoară aproape de frontiera externă a UE.

Pentru punerea în aplicare a agendei ambițioase pentru spațiul Schengen, stabilită în strategia din iunie 2021, Comisia a adoptat în luna mai primul raport privind starea spațiului Schengen[26]. Ciclul Schengen anual oferă un nou model de guvernanță pentru spațiul Schengen, cu un bilanț periodic al stării spațiului Schengen. Acesta va contribui la identificarea promptă a deficiențelor și a procedurilor eficiente de monitorizare, pentru un spațiu Schengen mai puternic și mai rezilient.

Acest prim raport recunoaște necesitatea de a consolida eforturile de punere în aplicare a inițiativelor-cheie la nivelul UE, inclusiv a verificărilor sistematice la frontierele externe pentru toți călătorii, utilizând pe deplin mandatele Frontex și Europol, precum și instrumentele de cooperare polițienească transfrontalieră propuse și disponibile.

În special, noua arhitectură a sistemelor de informații ale UE în materie de frontiere, migrație și securitate, precum și interoperabilitatea acestora reprezintă baza eforturilor de îmbunătățire a securității interne și a gestionării frontierelor. Punerea în aplicare efectivă a tuturor elementelor cadrului de interoperabilitate în conformitate cu termenele convenite va fi esențială.

Vigilență și coordonare

O cooperare mai strânsă în materie de aplicare a legii între statele membre și cu țările terțe este esențială pentru a asigura conștientizarea amenințărilor infracționale și teroriste emergente, precum și acțiuni împotriva rețelelor infracționale și a persoanelor care ar putea încerca să profite de războiul împotriva Ucrainei. Statele membre și partenerii operaționali fac în mod activ schimb de informații relevante disponibile și de date operative în materie penală cu Europol, care verifică și analizează informațiile și le transformă în notificări de informații operaționale pe baza cărora se pot întreprinde acțiuni, cum ar fi notificările de alertă timpurie și evaluările amenințărilor, care sunt partajate cu partenerii.

Criminalitatea organizată

Criminalitatea organizată găsește deja modalități de exploatare a situației actuale. Analiza inițială a informațiilor a identificat modele de criminalitate într-o serie de domenii, inclusiv traficul de persoane, declarațiile false privind mărfurile importate și exportate, frauda online, criminalitatea cibernetică și traficul de arme de foc. De asemenea, există dovezi privind faptul că infractorii cibernetici se erijează în filantropi care strâng fonduri pentru Ucraina cu scopul de a fura bani și criptomonede[27]. Organizațiile criminale din Ucraina pot încerca să se mute din cauza situației actuale și să își desfășoare activitățile în UE.

Comisia și președinția franceză a Consiliului au colaborat, implicând totodată și agențiile JAI ale UE, în special Europol, pentru a mobiliza Platforma multidisciplinară europeană împotriva amenințărilor infracționale (**EMPACT**), cu scopul de a evalua, a anticipa, a

[26] COM(2022) 301.

[27] Grupul Google de analiză a amenințărilor a observat că un număr tot mai mare de entități care reprezintă o amenințare folosesc războiul din Ucraina ca momeală în campaniile de phishing și malware. Cercetătorii de la compania de securitate a internetului Cyren raportează o creștere a înșelăciunilor criptografice care profită de conflict, utilizând site-uri false de donații.

preveni și a contracara amenințările existente sau emergente reprezentate de formele grave de criminalitate și de criminalitatea organizată. La 7 aprilie 2022, Europol a găzduit o reuniune EMPACT care a reunit reprezentanți și experți din statele membre ale UE și din comunitatea de securitate a UE pentru a se concentra asupra amenințărilor reprezentate de formele grave de criminalitate și de criminalitatea organizată care au apărut ca urmare a războiului din Ucraina. Printre măsurile concrete discutate s-au numărat colectarea mai multor informații, punerea în aplicare a acțiunilor operaționale de urgență și reorientarea celor existente, precum și zile de acțiune comună ad-hoc.

CELBET (echipa de experți vamali la frontierele terestre estice și sud-estice), proiect de colaborare finanțat de Comisia Europeană, urmărește evoluțiile de la frontieră în cadrul misiunii sale de a oferi sprijin operațional și îndrumare funcționarilor vamali și monitorizează confiscările vamale la punctele de trecere a frontierei UE (Polonia, Slovacia, Ungaria și România) cu Ucraina.

Activități infracționale și teroriste

Deși în UE nu a apărut încă nicio amenințare teroristă imediată în legătură cu invadarea Ucrainei de către Rusia, necesitatea vigilenței este evidentă.

Riscurile crescute de activități infracționale și teroriste evidențiază că este important ca statele membre să utilizeze bazele de date relevante ale UE, cum ar fi Sistemul de Informații Schengen, să introducă date în acestea, dacă este cazul, și să le consulte în timpul verificărilor efectuate asupra persoanelor care intră în UE. Acest lucru va contribui la asigurarea faptului că persoanele care reprezintă o amenințare la adresa securității interne a UE sunt identificate la frontierele externe. eu-LISA, Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție, continuă să asigure disponibilitatea și eficiența deplină a sistemelor UE de gestionare a frontierelor. Orientările[28] adresate statelor membre au clarificat modul în care se poate echilibra necesitatea de a asigura o bună gestionare a sosirilor la frontierele externe cu efectuarea simultană a controalelor de securitate necesare.

Pregătirea

Pe lângă orientare și coordonare, pregătirea UE a fost consolidată prin detașarea personalului agențiilor UE.

Europol a detașat echipe operaționale în statele membre ale UE care se învecinează cu Ucraina. Aceste echipe sunt formate din agenți invitați ai Europol din statele membre și experți Europol în Ungaria, Lituania, Polonia, România și Slovacia, precum și în Moldova[29]. Agenții invitați ai Europol sprijină autoritățile naționale în ceea ce privește controalele de securitate secundare la frontierele externe ale UE. Experții Europol oferă sprijin prin colectarea și evaluarea informațiilor pentru a detecta amenințările teroriste și infracționale, a sprijini anchetele și a identifica persoanele care prezintă risc din cauza tentativei de intrare în

[28] Comunicarea Comisiei – Furnizarea de orientări operaționale pentru gestionarea frontierelor externe în vederea facilitării trecerii frontierelor dintre Ucraina și UE, 2022/C 104 I/01.

[29] Începând cu 3 mai, Europol a detașat 1 membru al personalului Europol și 3 agenți invitați în Slovacia, 1 agent Europol în Polonia, 1 agent Europol și 4 agenți invitați în România și 2 agenți invitați în Ungaria. În Moldova, sunt detașați 1 membru al personalului Europol și 2 ofițeri invitați.

UE. Aceste echipe operaționale colectează informații care contribuie la evaluările amenințărilor infracționale, aflate la dispoziția statelor membre. O astfel de activitate de colectare de informații permite Europol să anticipeze evoluțiile și să coordoneze activitățile operaționale cu statele membre ale UE pentru a răspunde la activitățile grupurilor infracționale care încearcă să profite de războiul din Ucraina, precum și să valorifice angajamentul activ al Europol față de autoritățile ucrainene de aplicare a legii prin intermediul ofițerului de legătură ucrainean prezent la sediul Europol din Țările de Jos.

Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (**Frontex**) este, de asemenea, prezentă în statele membre și în țările vecine ale UE pentru a sprijini operațiunile de control la frontiere: în prezent, peste 2 100 de polițiști de frontieră sunt detașați în întreaga UE, în Balcanii de Vest și în Moldova. **Biroul European de Sprijin pentru Azil (EUAA)** a detașat aproape 750 de membri ai personalului în statele membre din sudul UE și în Lituania pentru a sprijini activitățile operaționale, a consolida capacitățile de primire și a contribui la procedurile de azil.

Pe baza actualei **Decizii Prüm**[30], care oferă statelor membre un cadru prin care pot detașa agenți de aplicare a legii pentru operațiuni comune, cum ar fi patrulele comune, Comisia și președinția franceză a Consiliului Uniunii Europene au transmis o scrisoare comună tuturor statelor membre pentru a identifica nevoile și a solicita detașarea de agenți de poliție, în scopul de a inițiа patrule comune în statele membre ale UE din prima linie care sunt cele mai afectate de trecerile în masă ale frontierei ca urmare a războiului. Comisia va finanța aceste detașări prin Fondul pentru securitate internă - componenta de cooperare polițienească.

Combaterea traficului de persoane

UE a fost în stare de alertă încă din primele zile ale războiului cu privire la riscurile unui anumit domeniu de activitate infracțională care ar putea profita de mișcările enorme de persoane care caută siguranță în UE. A fost esențial să se prevină ca, folosindu-se, de exemplu, de oferte false de transport sau de cazare, traficanții de persoane să vizeze persoanele vulnerabile care se deplasează, care sunt în principal **femei și copii**.

În martie, Europol și Eurojust au emis notificări de alertă timpurie către autoritățile naționale competente cu privire la potențialul trafic de persoane și exploatarea victimelor care sosesc din Ucraina. Eurojust contribuie la intensificarea schimbului de informații și la accelerarea cooperării judiciare, inclusiv cu Ucraina, iar anchetele privind traficul de persoane au fost transmise agenției în vederea coordonării.

Coordonatorul UE pentru combaterea traficului de persoane a organizat reuniuni cu Rețeaua UE de raportori naționali și mecanisme echivalente, cu agențiile din domeniul justiției și afacerilor interne și cu Platforma societății civile a UE de combatere a traficului de persoane, pentru a face schimb de informații cu privire la acțiunile necesare pentru prevenirea și combaterea abuzurilor și pentru protejarea victimelor. Au fost deschise anchete în mai multe state membre cu privire la potențiale cazuri.

[30] 2008/615/JAI, 2008/616/JAI.

UE a acționat rapid și energic în a asigura un răspuns coordonat la această amenințare reală la adresa persoanelor care au nevoie de ajutorul UE. Orientări operaționale[31], inclusiv cu privire la provocarea reprezentată de traficul de persoane, au fost puse rapid la dispoziția statelor membre care pun în aplicare Directiva privind protecția temporară, cu scopul de a oferi sprijin persoanelor care fug din calea războiului din Ucraina. Ca parte a Planului în 10 puncte pentru o coordonare europeană mai puternică cu privire la primirea persoanelor care fug din calea războiului din Ucraina[32], prezentat în cadrul Consiliului Justiție și Afaceri Interne din 28 martie 2022, coordonatorul UE pentru combaterea traficului de persoane, în cooperare cu agențiile UE și cu statele membre, a elaborat un plan comun de combatere a traficului de persoane[33] privind prevenirea traficului de persoane și sprijinirea victimelor. Înregistrarea entităților și a persoanelor (inclusiv a voluntarilor) care intenționează să ofere cazare, transport și alte tipuri de asistență, precum și efectuarea de verificări ale antecedentelor reprezintă un aspect deosebit de important. De asemenea, Comisia a luat legătura cu EUAA pentru a sprijini depistarea victimelor traficului de persoane atunci când sunt efectuate examinări medicale în centrele de primire. Copiii neînsoțiți sau separați de familie sunt expuși unui risc deosebit de abuz, de exploatare sexuală sau de criminalitate forțată. Orientările operaționale menționate mai sus prevăd, de asemenea, îndrumări pentru a ajuta statele membre să gestioneze sosirea, primirea și sprijinul acordat copiilor și, în special, minorilor neînsoțiți. Pentru a sensibiliza persoanele expuse riscului, Comisia a lansat, de asemenea, un site web specific, cu o secțiune care include recomandări practice privind modul în care să se evite traficanții.

Deși unele acțiuni de sporire a gradului de pregătire au fost întreprinse în special ca răspuns la noile condiții generate de război, alte măsuri-cheie decurg din **inițiativele legislative** aflate deja în curs de elaborare înainte de războiul de agresiune al Rusiei împotriva Ucrainei.

Comisia salută acordul din februarie 2022 privind mandatul revizuit al **Europol**[34], care, odată pus în aplicare, va permite Europol să sprijine mai bine statele membre în lupta împotriva criminalității organizate și a terorismului. Astfel, agenția va dispune de instrumentele și garanțiile adecvate ca să sprijine forțele de poliție să analizeze volumele mari de date pentru investigarea infracțiunilor și să dezvolte metode inovatoare de combatere a criminalității cibernetice. Aceste schimbări sunt însoțite de un cadru consolidat de protecție a datelor, precum și de un grad mai mare de control parlamentar și de asumare a răspunderii.

Pachetul privind **cooperarea polițienească** prezentat de Comisie la 8 decembrie 2021[35], care este în curs de negociere, va consolida cooperarea între funcționarii însărcinați cu aplicarea legii din statele membre, făcând schimbul de date mai rapid, mai ușor și mai sigur, precum și consolidând și eficientizând cooperarea polițienească operațională pe teren. Comisia invită Parlamentul European și Consiliul să adopte rapid acest pachet.

[31] C/2022/1806, EUR-Lex - 52022XC0321(03) - RO - EUR-Lex (europa.eu).
[32] https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en.
[33] https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en.
[34] COM(2020) 796.
[35] COM(2021) 780, COM(2021) 782, COM(2021) 784.

Odată adoptate și puse în aplicare, aceste propuneri legislative vor sprijini autoritățile de aplicare a legii în lupta împotriva criminalității organizate transfrontaliere. Acest lucru va fi deosebit de important într-un context în care organizațiile criminale din Ucraina pot încerca să se mute din cauza situației actuale și să își desfășoare activitățile în UE.

Misiunea de consiliere a UE în Ucraina sprijină reforma instituțiilor însărcinate cu asigurarea respectării legii și a instituțiilor statului de drept din această țară începând din 2014. În martie 2022, mandatul misiunii a fost revizuit, permițând acordarea de sprijin la punctele de trecere a frontierei ucrainene cu Polonia, România și Slovacia, contribuind la conștientizarea situației în ceea ce privește activitățile infracționale transfrontaliere, inclusiv traficul de persoane, și fluxul de bunuri umanitare în Ucraina.

IV. ARME, MATERIALE PERICULOASE ȘI INCIDENTE CRITICE

Războiul a sporit masiv circulația armelor de foc și a altor arme pe teritoriul Ucrainei, ceea ce prezintă noi riscuri pentru UE și alte state învecinate cu Ucraina.

Vigilență și coordonare

Orientările operaționale, emise în martie, oferă statelor membre recomandări cu privire la modul de abordare a provocării reprezentate de creșterea circulației armelor de foc într-o perioadă de sosiri în masă la frontiera externă a UE[36]. Aceste orientări subliniază faptul că prezența armelor de foc ar trebui verificată în permanență și că nicio persoană care nu are autorizație nu ar trebui să poată intra în UE cu o armă de foc. Atunci când autoritățile ucrainene raportează că lipsesc arme de foc, statele membre ar trebui să raporteze situația în Sistemul de Informații Schengen.

Este esențial ca toate transporturile de arme de foc către Ucraina să fie înregistrate în mod corespunzător, cu toate informațiile relevante (inclusiv tipul, țara și anul de fabricație, marca, modelul, calibrul, numărul de serie) pentru a facilita trasabilitatea respectivelor arme de foc, atât în Ucraina, cât și în UE.

UE a deplâns în mod public atacurile militare imprudente ale Rusiei asupra instalațiilor nucleare, biologice și chimice civile din Ucraina și din vecinătatea imediată a acestora, precum și orice act care compromit siguranța acestor instalații. Comisia monitorizează situația din Ucraina, acordând o atenție deosebită amenințării radiologice care reprezintă cea mai mare preocupare din punctul de vedere al securității interne a UE[37]. De asemenea, Comisia monitorizează potențialele amenințări chimice și a instituit un mecanism intern de coordonare în cazul în care este necesară o evaluare rapidă a riscurilor.

Pregătirea

Ucraina este deja una dintre țările identificate ca fiind esențiale pentru acțiuni specifice la nivel extern în Planul de acțiune al UE privind traficul de arme de foc pentru perioada 2020-2025. Există, de asemenea, o acțiune operațională specifică în regiune, inclusiv în

[36] Comunicare a Comisiei – Furnizarea de orientări operaționale pentru gestionarea frontierelor externe în vederea facilitării trecerii frontierelor dintre Ucraina și UE 2022/C 104 I/01.

[37] Comisia va organiza, în cooperare cu partenerii din SUA, un atelier axat pe riscurile legate de materialele radiologice aflate în spitalele care nu se mai află sub controlul reglementar.

Ucraina, în cadrul EMPACT – componenta privind armele de foc. Cu toate acestea, având în vedere riscurile de sustragere a armelor de foc, vor fi necesare proiecte specifice finanțate de UE, precum și o cooperare operațională cu Europol, Frontex și componenta privind armele de foc din cadrul EMPACT. Comisia va prezenta în curând o propunere de revizuire a Regulamentului privind armele de foc[38] în ceea ce privește exporturile, importurile și tranzitul de arme de foc pentru uz civil, ca parte a cadrului juridic și operațional general de prevenire, depistare, investigare și urmărire penală a traficului de arme de foc.

Pentru a îmbunătăți pregătirea și răspunsul UE la riscurile la adresa sănătății publice, cum ar fi amenințările CBRN, Comisia creează rezerve strategice de capacități de răspuns prin intermediul mecanismului de protecție civilă al UE (UCPM), finanțat de Autoritatea pentru Pregătire și Răspuns în caz de Urgență Sanitară (HERA)[39]. Serviciile Comisiei lucrează împreună la dezvoltarea unui stoc strategic rescEU în valoare de 540,5 milioane EUR. Acest stoc va fi alcătuit din echipamente și medicamente, vaccinuri și alte mijloace terapeutice pentru tratarea pacienților expuși la agenți CBRN, precum și dintr-o rezervă rescEU de decontaminare compusă din echipamente de decontaminare și echipe de intervenție specializate. Ca prim pas imediat, UE și-a mobilizat rezerva medicală rescEU pentru a achiziționa comprimate de iodură de potasiu care pot fi utilizate pentru a proteja persoanele împotriva efectelor nocive ale radiațiilor, precum și alte articole care sunt necesare de urgență în Ucraina. Aproape 3 milioane de comprimate de iodură au fost deja livrate Ucrainei prin intermediul UCPM, cu ajutorul Franței și al Spaniei.

V. ACȚIUNI COORDONATE PENTRU A TRAGE LA RĂSPUNDERE RUSIA CA URMARE A AGRESIUNII

UE joacă un rol decisiv în acțiunile comunității internaționale de a exercita presiuni asupra Rusiei ca aceasta să înceteze agresiunea inacceptabilă și contrară dreptului internațional împotriva statului ucrainean și a civililor prinși în conflict. Această presiune include măsuri de precizare a consecințelor pentru autorii agresiunii, inclusiv sancțiuni severe, precum și acțiuni de identificare și de facilitare a urmăririi penale a crimelor de război.

Măsuri restrictive și confiscare

De la recunoașterea, la 21 februarie 2022, de către Rusia a regiunilor ucrainene Donețk și Lugansk care nu se află sub controlul guvernului și de la invadarea Ucrainei, la 24 februarie 2022, UE a impus cea mai mare serie de măsuri restrictive adoptate vreodată împotriva Rusiei. Până în prezent, au fost adoptate cinci pachete de sancțiuni. Aceste măsuri se axează pe sectoare-cheie, printre care se numără finanțele, comerțul, transporturile, apărarea și mass-media, și vizează elite politice și militare, precum și oligarhi ruși și belaruși proeminenți. Listele includ deja peste 1 000 de persoane și 80 de entități. Un al șaselea pachet de sancțiuni este în curs de dezbatere în cadrul Consiliului.

---

[38] Regulamentul (UE) nr. 258/2012 al Parlamentului European și al Consiliului din 14 martie 2012 privind punerea în aplicare a articolului 10 din Protocolul Organizației Națiunilor Unite împotriva fabricării și traficului ilegale de arme de foc, piese și componente ale acestora, precum și de muniții, adițional la Convenția Organizației Națiunilor Unite împotriva criminalității transnaționale organizate (Protocolul ONU privind armele de foc) și de stabilire a măsurilor privind autorizațiile de export, importul și tranzitul pentru arme de foc, piese și componente ale acestora, precum și muniții.

[39] Planul de lucru al HERA pentru 2022 (europa.eu).

Impactul acestor măsuri restrictive și al măsurilor restrictive anterioare împotriva persoanelor și întreprinderilor ruse și belaruse va fi proporțional cu punerea lor în aplicare. Coordonarea la nivelul UE poate aduce o contribuție majoră la eliminarea eventualelor breșe, iar Comisia oferă un sprijin amplu părților interesate, prin orientări scrise, reuniuni ale părților interesate și un grup special de experți, precum și printr-o serie de resurse menite să faciliteze conformitatea.

În plus, Comisia a înființat un grup operativ „Înghețare și punere sub sechestru", care reunește serviciile Comisiei, statele membre, Eurojust și Europol. Până la momentul actual, statele membre au raportat că au înghețat active în valoare de 9,89 miliarde EUR[40]. La 11 aprilie, Europol, împreună cu statele membre, Eurojust și Frontex, a lansat operațiunea Oscar pentru a sprijini anchetele financiare și anchetele penale care vizează activele provenite din săvârșirea de infracțiuni deținute de persoane fizice și de entități juridice care fac obiectul sancțiunilor UE legate de războiul Rusiei împotriva Ucrainei. Grupul operativ al UE „Înghețare și punere sub sechestru" colaborează îndeaproape cu Grupul operativ „Russian Elites, Proxies, and Oligarchs (REPO)" (Elite, împuterniciți și oligarhi ruși), înființat de țările G7 (Canada, Franța, Germania, Italia, Japonia, Regatul Unit, Statele Unite) și cu parteneri care împărtășesc aceeași viziune, cum ar fi Australia, precum și cu Grupul operativ „KleptoCapture" al SUA și cu grupul operativ ucrainean.

Grupul operativ „Înghețare și punere sub sechestru" servește drept platformă pentru coordonarea și facilitarea schimbului de informații și de experiență între statele membre și furnizarea de orientări cu privire la punerea în aplicare a sancțiunilor, precum și pentru facilitarea schimbului de bune practici privind anchetele penale și confiscarea. În special, este important ca autoritățile de aplicare a legii să fie vigilente și proactive în legătură cu potențialele infracțiuni comise de persoanele și entitățile care fac obiectul sancțiunilor. Grupul operativ urmărește, de asemenea, să aducă în discuție posibila utilizare a fondurilor confiscate, de exemplu pentru a contribui la reconstrucția Ucrainei.

Comisia adoptă astăzi un pachet privind **recuperarea și confiscarea activelor**[41], care ia în considerare lecțiile învățate din punerea în aplicare a măsurilor restrictive ale Uniunii împotriva persoanelor și entităților ruse și belaruse. Acesta va facilita punerea în aplicare eficace a măsurilor restrictive ale UE în întreaga Uniune, permițând urmărirea și identificarea rapidă a bunurilor deținute sau controlate de persoane sau entități care fac obiectul unor astfel de măsuri. Cadrul consolidat privind recuperarea și confiscarea activelor se va aplica, de asemenea, încălcării măsurilor restrictive și, prin urmare, va asigura urmărirea, înghețarea, gestionarea și confiscarea eficace a produselor provenite din încălcarea măsurilor restrictive. Pentru a se asigura că activele persoanelor și entităților care încalcă măsurile restrictive pot fi efectiv confiscate, Comisia adoptă, de asemenea, astăzi o propunere de decizie a Consiliului de a adăuga încălcarea sancțiunilor pe lista UE de infracțiuni de la articolul 83 alineatul (1) din TFUE[42], însoțită de o comunicare[43], în vederea propunerii unei directive de apropiere a definiției infracțiunilor și a sancțiunilor pentru încălcarea măsurilor restrictive.

La modul mai general, acest pachet marchează un pas crucial în lupta împotriva criminalității organizate. Acesta vine ca urmare a angajamentelor asumate de Comisie în cadrul Strategiei

[40] De asemenea, sunt blocate active ale Băncii Centrale a Rusiei în valoare de aproximativ 23 de miliarde EUR.
[41] COM(2022) 245.
[42] COM(2022) 247.
[43] COM(2022) 249.

privind o uniune a securității și al Strategiei de combatere a criminalității organizate 2020-2025[44]. Acest pachet revizuiește Directiva din 2014 privind confiscarea, Decizia Consiliului din 2007 privind birourile de recuperare a activelor (ARO) și Decizia-cadru din 2005 privind confiscarea produselor, a instrumentelor și a bunurilor având legătură cu infracțiunea, pentru a consolida capacitățile de urmărire și identificare și, în cele din urmă, de confiscare a câștigurilor ilicite, abordând ratele foarte scăzute de confiscare din UE[45]. Pachetul extinde domeniul de aplicare privind infracțiunile vizate și normele privind confiscarea în cazurile în care o condamnare penală pentru o anumită infracțiune nu este posibilă, dar în care activele provin în mod clar din activități infracționale. Revizuirea consolidează, de asemenea, gestionarea eficace a activelor înghețate și confiscate și consolidează capacitatea birourilor de recuperare a activelor de a urmări și a identifica activele ilicite. Noul cadru al UE privind recuperarea activelor este conceput pentru a aborda modul complex de operare al organizațiilor criminale, care operează frecvent la nivel transfrontalier și utilizează diverse metode pentru a-și ascunde activele, inclusiv prin intermediul criptoactivelor.

Răspunsul judiciar coordonat

De asemenea, la nivelul UE s-au depus eforturi pentru a se asigura un răspuns judiciar coordonat la **crimele internaționale** potențial comise în Ucraina, astfel încât autorii acestora să poată fi trași la răspundere.

Două state membre și Ucraina au înființat o echipă comună de anchetă (JIT) pentru a investiga crimele de război, crimele împotriva umanității și alte crime internaționale potențial comise pe teritoriul Ucrainei. Eurojust oferă sprijin juridic, analitic, financiar și logistic acestei echipe comune de anchetă. La 25 aprilie 2022, Parchetul Curții Penale Internaționale (OTP-CPI) s-a alăturat echipei comune de anchetă, în calitate de participant, și se preconizează că și alți participanți se vor alătura curând[46].

La 25 aprilie 2022, Comisia a prezentat o propunere de modificare a Regulamentului privind Eurojust[47] pentru ca Eurojust să păstreze, să analizeze și să stocheze probe privind principalele infracțiuni internaționale. Eurojust și Europol vor continua să colaboreze îndeaproape pe parcursul acestui proces. Un rol esențial în coordonarea răspunsului judiciar este jucat, de asemenea, de Rețeaua privind genocidul, al cărei secretariat este asigurat de Eurojust. Aceasta a pregătit un atlas al ONG-urilor active în prezent în Ucraina și sprijină practicienii naționali din statele membre și Ucraina care tratează cazuri active legate de război.

În aprilie 2022, Consiliul a revizuit din nou mandatul **Misiunii UE de consiliere în Ucraina**, deschizând calea pentru sprijinirea de către misiune a autorităților ucrainene în ceea ce privește anchetarea și urmărirea penală a eventualelor crime internaționale comise în contextul agresiunii militare a Rusiei. Misiunea va oferi autorităților ucrainene consiliere strategică cu privire la anchetarea și urmărirea penală a crimelor internaționale, la modificările necesare ale legislației ucrainene, la strategia de comunicare, precum și la

[44] COM(2021) 170.

[45] Europol estimează că doar 2 % din activele provenite din săvârșirea de infracțiuni sunt înghețate (2,4 miliarde EUR), iar 1 % confiscate (1,2 miliarde EUR), în timp ce veniturile provenite din săvârșirea de infracțiuni pe principalele piețe infracționale din UE s-au ridicat la 139 de miliarde EUR în 2019 (1 % din PIB-ul UE).

[46] https://www.eurojust.europa.eu/eurojust-and-the-_war-in-ukraine.

[47] COM(2022) 187 final.

formarea pe teme conexe. Misiunea face parte dintr-o serie de inițiative de coordonare în acest context și, împreună cu delegația UE, face parte din Grupul consultativ SUA-UE privind atrocitățile din Ucraina.

VI. ACȚIUNI STRĂINE DE MANIPULARE A INFORMAȚIILOR ȘI INGERINȚE STRĂINE

Evoluțiile geopolitice actuale subliniază riscurile de ingerințe străine. Agresiunea militară a Rusiei împotriva Ucrainei este însoțită de activități de **manipulare a informațiilor și de ingerință**. Au fost lansate acuzații nefondate de „nazism" și „genocid" împotriva guvernului ucrainean, operațiuni de inducere în eroare și acuzații nefondate împotriva NATO și a Occidentului pentru a justifica atacurile brutale asupra Ucrainei, concomitent cu suprimarea libertății de exprimare și a relatărilor independente în interiorul Rusiei. Există în continuare un risc de manipulare a materialelor audiovizuale și de dezinformare pe care Rusia ar putea încerca să le utilizeze ca pretext pentru atacuri militare suplimentare, pentru a slăbi hotărârea rezistenței ucrainene, pentru a diviza comunitatea internațională în ceea ce privește opoziția sa față de război sau pentru a cultiva îndoiala cu privire la încălcările dreptului internațional de către Rusia. În cadrul Busolei strategice, UE s-a angajat să răspundă ferm la acțiunile străine de manipulare a informațiilor și la ingerințele străine și să își consolideze reziliența și capacitatea de a contracara astfel de amenințări[48]. Manipularea dezbaterii democratice în interiorul UE face obiectul Planului de acțiune pentru democrația europeană, planul coordonat al Comisiei de combatere a dezinformării și de consolidare a rezilienței democratice[49].

Vigilență și coordonare

Uniunea Europeană a răspuns printr-o acțiune decisivă și coordonată la campania de dezinformare a Rusiei în contextul agresiunii militare împotriva Ucrainei. UE colaborează îndeaproape cu statele sale membre prin intermediul sistemului de alertă rapidă și cu parteneri internaționali, cum ar fi NATO, SUA, Canada și mecanismul de reacție rapidă al G7, pentru a face schimb de informații cu privire la tendințele și tacticile de manipulare utilizate de Kremlin. Eforturile de deconstrucție a manipulărilor Kremlinului s-au intensificat, în special prin intermediul site-ului web EUvsDisinfo, care transmite în limbile engleză, rusă, ucraineană și în alte limbi, pentru a furniza informații concrete în interiorul UE, în Ucraina și în regiune, precum și în Rusia. Începând cu 2 martie, transmisia și difuzarea canalelor RT și Sputnik ale mass-mediei de stat ruse în UE sau direcționate către UE au fost suspendate, ca urmare a măsurilor restrictive adoptate de UE. Platformele online, principalele rețele sociale, agențiile de publicitate și sectorul publicității care sunt semnatari ai Codului de bune practici privind dezinformarea[50] iau măsuri urgente pentru a limita dezinformarea legată de agresiunea Rusiei împotriva Ucrainei. Comisia și SEAE monitorizează aceste eforturi. Informațiile furnizate arată că platformele și-au consolidat instrumentele de monitorizare și de intervenție legate de război.

[48] https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/ro/pdf.
[49] COM(2020) 790.
[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

În plus, sunt puse în aplicare rapid acțiuni pentru a sprijini țările din Asia Centrală și din Balcanii de Vest să își consolideze reziliența în materie de informații și să combată acțiunile străine de manipulare a informațiilor și ingerințele străine.

Pregătirea

Utilizarea excesivă a acțiunilor străine de manipulare a informațiilor și a ingerințelor străine (FIMI), inclusiv a dezinformării, ca unul dintre instrumentele amenințărilor hibride, a dat un nou caracter urgent acțiunilor subsecvente Planului de acțiune pentru democrația europeană. În ultimele luni, instituțiile UE au sprijinit statele membre în combaterea FIMI, în special în cadrul sistemului de alertă rapidă, prin schimbul de informații cu privire la tacticile utilizate de actorii FIMI și la strategiile de răspuns. Sunt în desfășurare dezbateri pentru consolidarea în continuare a răspunsului general al UE la FIMI, pe baza unui document de reflecție prezentat de SEAE cu privire la elaborarea unui **set de instrumente** specific pentru abordarea acestei amenințări. Acesta reunește măsurile interne existente și noile instrumente ale UE din cadrul politicii externe și de securitate comune. De asemenea, dezbaterile vor beneficia de acțiunea intensificată a Stratcom din cadrul Serviciului European de Acțiune Externă[51], precum și a Comisiei.

Observatorul european al mass-mediei digitale („EDMO") a instituit un grup operativ privind dezinformarea în urma izbucnirii războiului din Ucraina și coordonează acțiunile verificatorilor veridicității informațiilor și ale cercetătorilor din rețeaua sa. Acesta a analizat modul în care cei care susțin teoria conspirației COVID-19 au pivotat rapid în direcția diseminării de informații false pro-ruse, schimbare observată în mai multe state membre[52].

Propunerea de act legislativ privind serviciile digitale urmărește adaptarea la tehnologiile digitale care evoluează rapid și la ceea ce înseamnă acest lucru în materie de provocări tehnologice și democratice, cum ar fi discursurile de incitare la ură, dezinformarea online și strategiile de destabilizare. Progresele semnificative înregistrate în cadrul negocierilor desfășurate de Parlamentul European și Consiliu ar trebui să permită adoptarea rapidă a pachetului.

VII. O PREGĂTIRE MAI AMPLĂ

Într-un moment în care războiul s-a întors în Europa, precum și într-o perioadă de schimbări geopolitice majore, coordonarea securității în UE s-a intensificat, bazându-se pe inițiativele aflate deja în curs de pregătire înainte de izbucnirea războiul de agresiune al Rusiei împotriva Ucrainei. Inițiativele care vizează în principal securitatea externă a UE au implicații puternice pentru agenda internă a uniunii securității.

[51] Serviciul Comunicare strategică, grupuri operative și analiză a informațiilor din cadrul Serviciului European de Acțiune Externă oferă sprijin pentru comunicarea strategică în punerea în aplicare a politicii externe și de securitate a UE în regiunile prioritare conexe (vecinătatea sudică și estică, Balcanii de Vest), prin dezvoltarea și punerea în aplicare a unor acțiuni specifice de comunicare strategică axate pe promovarea politicilor, valorilor, obiectivelor și intereselor UE.

[52] https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/.

La 15 februarie 2022, Comisia a prezentat **pachetul privind apărarea**[53], conținând o serie de inițiative în domenii critice pentru apărare și securitate în cadrul UE. Această contribuție a Comisiei la apărarea și securitatea europene acoperă întreaga gamă de provocări. Pachetul propune măsuri concrete în direcția unei piețe europene a apărării mai integrate și mai competitive, în special prin consolidarea cooperării în cadrul UE și prin crearea unor economii de scară. Totodată, acesta este însoțit de o foaie de parcurs privind tehnologiile critice pentru securitate și apărare, cu scopul de a promova cercetarea, dezvoltarea tehnologică și inovarea în aceste sectoare și de a reduce dependențele în ceea ce privește tehnologiile critice și lanțurile valorice. Pachetul vizează, de asemenea, consolidarea dimensiunii de apărare a spațiului la nivelul UE. În plus, acesta analizează modul în care Comisia ar putea să își intensifice acțiunile împotriva amenințărilor hibride, inclusiv în domeniul cibernetic, să își sporească mobilitatea militară în interiorul și în afara Europei și să abordeze în continuare provocările reprezentate de schimbările climatice în materie de apărare. Pentru a completa această activitate, Comunicarea comună privind **analiza deficitelor de investiții în domeniul apărării și calea de urmat**[54] din 18 mai analizează deficitele în materie de capabilități și de industrie care trebuie abordate în vederea sprijinirii celor mai expuse state membre ale UE și a identificării măsurilor de atenuare a deficiențelor identificate.

Reziliența UE la aceste amenințări implică, de asemenea, abordări bazate pe capabilități în toate sectoarele de securitate, astfel cum se susține în Planul de acțiune al Comisiei privind sinergiile dintre industria civilă, industria de apărare și industria spațială[55]. Se lucrează la promovarea abordărilor bazate pe capabilități în domeniul securității interne și al asigurării respectării legii.

La 21 martie 2022, Consiliul a adoptat **Busola strategică pentru securitate și apărare**[56], aprobată la scurt timp de Consiliul European. Busola prezintă un plan de acțiune ambițios pentru consolidarea politicii de securitate și apărare a UE până în 2030. Obiectivul este de a face din UE un furnizor de securitate mai puternic și mai capabil, care să își protejeze cetățenii și să contribuie la pacea și securitatea internaționale. Aceasta conține propuneri concrete, cu un calendar foarte precis de punere în aplicare, pentru îmbunătățirea capacității UE de a acționa în mod decisiv în situații de criză.

Unul dintre rezultatele Busolei strategice constă în dezvoltarea unui set de **instrumente hibride ale UE** care ar trebui să ofere un cadru pentru un răspuns coordonat la campaniile hibride care afectează UE și statele sale membre, incluzând măsuri interne și externe. În urma procesului de identificare a valorilor de referință sectoriale în materie de reziliență, care a avut loc la începutul anului 2022[57], va fi finalizată o analiză a deficitelor și a nevoilor. În acest cadru, UE va continua să consolideze pregătirea, reziliența și răspunsul la amenințările generate de agresiunea Rusiei și la orice alte încercări de destabilizare a democrațiilor și a ordinii multilaterale bazate pe norme.

---

[53] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en.

[54] JOIN(2022) 24.

[55] COM(2021) 70.

[56] O Busolă strategică pentru securitate și apărare – Pentru o Uniune Europeană care își protejează cetățenii, valorile și interesele și contribuie la pacea și securitatea internaționale: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/ro/pdf.

[57] SWD(2022) 21 final.

VIII. PERSPECTIVE

Privind în perspectivă, UE va trebui să rămână extrem de vigilentă la amenințările în continuă evoluție și să își consolideze **pregătirea și reziliența pentru orice eventualitate**. Repercusiunile războiului pot lua forme diferite și nu toate pot fi evaluate la momentul actual.

Amploarea strămutării rețelelor infracționale ucrainene încă nu este cunoscută. Activitatea anterioară a Eurojust indică o tendință de trafic de heroină din Afganistan către UE prin Ucraina, astfel cum a fost confirmată de Observatorul European pentru Droguri și Toxicomanie (OEDT)[58]. Instabilitatea poate îngreuna acțiunile de combatere a comerțului cu heroină pe această rută, generând riscul unei posibile creșteri a fluxului de droguri către UE.

Este mai probabil ca unele riscuri pentru UE să se intensifice la sfârșitul luptelor sau în timpul eventualelor pauze. Se va acorda o atenție deosebită circulației armelor de foc, riscul crescând atunci când luptele din Ucraina vor fi mai puțin intense. Experiența anterioară indică, de asemenea, riscul ca întoarcerea luptătorilor străini care au dobândit experiență în luptă și care ar fi putut intra în contact cu grupuri extremiste să poată duce la acte teroriste în UE într-o etapă ulterioară. Acest fenomen potențial ar trebui monitorizat cu atenție, iar Comisia facilitează deja discuțiile între statele membre cu privire la provocările generate de întoarcerea voluntarilor străini cu antecedente extremiste violente.

Având în vedere aceste posibile amenințări, este important ca punerea în aplicare a Strategiei privind o uniune a securității să continue, inclusiv prin punerea în aplicare a unor strategii-cheie, cum ar fi Strategia de securitate cibernetică a UE, Strategia de combatere a criminalității organizate (2020-2025), Agenda UE privind combaterea terorismului (2020-2025), Planul de acțiune al UE privind traficul de arme de foc (2020-2025), Strategia UE privind combaterea traficului de persoane (2021-2025) și Strategia UE în materie de droguri (2021-2025).

Vor continua eforturile de a oferi Uniunii Europene cadrul legislativ necesar. De exemplu, Comisia pregătește evaluarea impactului pentru o propunere de reglementare a comercializării și utilizării substanțelor chimice cu grad ridicat de risc.

IX. CONCLUZIE

Uniunea securității continuă să își joace rolul în pregătirea UE și a statelor sale membre pentru ca acestea să facă față amenințărilor existente și potențiale. Războiul Rusiei de agresiune împotriva Ucrainei a demonstrat cât de repede pot deveni reale amenințările teoretice și subliniază importanța vigilenței, a coordonării și a pregătirii.

[58] „Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data)" [Raport privind situația drogurilor și a alcoolului în Ucraina pentru 2020 (conform datelor din 2019)], OEDT; „Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery" (Stoparea traficului cu un înlocuitor de heroină în Franța, Polonia și Ucraina, inclusiv planificarea și executarea unei livrări supravegheate), 2021/00446, Eurojust, mai 2020.

Acest al patrulea raport referitor la Strategia privind o uniune a securității demonstrează că UE este capabilă să se adapteze, chiar și în fața unor amenințări excepționale și neprevăzute, cum ar fi cele generate de războiul de agresiune al Rusiei împotriva Ucrainei. Punerea cu hotărâre în aplicare a Strategiei privind o uniune a securității este mai importantă ca niciodată.