Consiliul
Uniunii Europene

Bruxelles, 22 mai 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Destinatar:	Delegațiile
Nr. doc. ant.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Subiect:	Concluziile Consiliului privind politica UE în domeniul apărării cibernetice

În continuare, se pun la dispoziția delegațiilor Concluziile Consiliului privind politica UE în domeniul apărării cibernetice, astfel cum au fost aprobate de Consiliu în cadrul reuniunii sale desfășurate la 22 mai 2023.

Concluziile Consiliului privind politica UE în domeniul apărării cibernetice

1. Luând ca bază Cadrul de politici pentru apărarea cibernetică din 2014 și actualizarea acestuia din 2018, Consiliul salută ambițioasa Comunicare comună privind politica UE în domeniul apărării cibernetice pentru a investi în continuare în forțele noastre armate moderne și interoperabile, în tehnologii de vârf și în capabilități de apărare cibernetică de ultimă generație, precum și pentru a consolida parteneriatele în vederea abordării provocărilor comune. Spațiul cibernetic a devenit un domeniu de concurență strategică, într-un moment în care dependența de tehnologiile digitale este din ce în ce mai mare. Astfel, este esențial să se mențină un spațiu cibernetic deschis, liber, stabil și securizat. Recurgerea la operațiuni cibernetice care au înlesnit și au însoțit războiul de agresiune neprovocat și nejustificat al Rusiei împotriva Ucrainei afectează stabilitatea și securitatea mondială, reprezintă un risc important de escaladare și se adaugă creșterii deja semnificative, în ultimii ani, a activităților cibernetice răuvoitoare în afara contextului conflictelor armate.

2. Războiul din Ucraina a creat un nou context strategic și a confirmat necesitatea ca UE, statele sale membre și partenerii lor să consolideze în continuare reziliența UE pentru a face față amenințărilor cibernetice și pentru a spori securitatea noastră cibernetică comună și apărarea noastră cibernetică comună împotriva comportamentelor răuvoitoare și a actelor de agresiune în spațiul cibernetic. Comunicarea comună privind politica UE în domeniul apărării cibernetice semnalează hotărârea noastră de a oferi măsuri imediate și pe termen lung pentru a asigura libertatea de acțiune în spațiul cibernetic și pentru a da o ripostă actorilor care generează amenințări care urmăresc, printre altele, să pătrundă, să perturbe sau să distrugă rețelele și sistemele informatice ale UE și ale partenerilor săi. În completarea Strategiei de securitate cibernetică a UE și în concordanță cu Busola strategică, această comunicare comună reprezintă un pas semnificativ către abordarea UE care acoperă întregul spectru în ceea ce privește reziliența, răspunsul, prevenirea conflictelor, cooperarea și stabilitatea în spațiul cibernetic. În acest context, Consiliul subliniază necesitatea unor răspunsuri adecvate și coerente din partea UE, a statelor sale membre și a partenerilor lor, așteptând, totodată, cu interes revizuirea orientărilor privind punerea în aplicare a setului de instrumente pentru diplomația cibernetică al UE, aceasta fiind o altă etapă importantă în evoluția posturii de securitate cibernetică a UE.

3. Consiliul subliniază că recentele atacuri cibernetice împotriva infrastructurii critice europene, evoluția rapidă a situației amenințărilor cibernetice și ritmul accelerat al evoluțiilor tehnologice demonstrează, de asemenea, necesitatea unei cooperări și coordonări civil-militare consolidate, subliniind, în același timp, că nu există o ierarhie între comunitățile civile și militare.
   Politica UE în domeniul apărării cibernetice permite UE și statelor sale membre să își consolideze capacitatea de protejare, detectare, apărare și descurajare, utilizând în mod adecvat întreaga gamă de opțiuni de apărare care se află la dispoziția comunităților civile și militare în scopul mai amplu al securității și apărării UE, în conformitate cu dreptul internațional, inclusiv cu dreptul drepturilor omului și cu dreptul internațional umanitar.

4. Deși securitatea națională, inclusiv în domeniul cibernetic, rămâne responsabilitatea exclusivă a fiecărui stat membru, astfel cum este prevăzut la articolul 4 alineatul (2) din TUE, Consiliul subliniază, totodată, necesitatea realizării unor investiții substanțiale, în mod individual și în colaborare, în consolidarea rezilienței și în desfășurarea întregului spectru de capabilități de apărare cibernetică și mobilizând cadrele de cooperare și stimulentele financiare ale UE. Consiliul subliniază necesitatea consolidării în continuare a acțiunilor statelor membre și ale instituțiilor, organelor și agențiilor UE (IOAUE) pentru a proteja Uniunea, cetățenii noștri, IOAUE și misiunile și operațiile PSAC în spațiul cibernetic. În plus, acesta subliniază importanța rezilienței UE în spațiul cibernetic prin dezvoltarea capabilităților de apărare cibernetică și prin consolidarea cooperării cu un ecosistem privat de încredere.

I. **Acțiuni comune pentru o apărare cibernetică mai puternică**

5. Consiliul reafirmă că un proces progresiv, transparent și incluziv este esențial pentru sporirea încrederii, care are un rol central în elaborarea în continuare a unui cadru al UE de gestionare a crizelor în materie de securitate cibernetică, care urmează să fie realizată în concordanță cu Foaia de parcurs privind gestionarea crizelor cibernetice elaborată în cadrul Consiliului. Consiliul reafirmă necesitatea de a ne spori în continuare capacitatea de protejare împotriva atacurilor cibernetice, de detectare a acestora, de apărare împotriva lor și de descurajare a lor printr-o conștientizare îmbunătățită a situației, prin consolidarea capacităților, prin dezvoltarea capabilităților, prin formare, prin exerciții și printr-o reziliență consolidată și printr-un răspuns ferm la atacurile cibernetice împotriva UE, a statelor sale membre, a IOAUE, a misiunilor și operațiilor PSAC, utilizând toate mijloacele adecvate. În acest sens, Consiliul încurajează Înaltul Reprezentant și Comisia să reducă complexitatea în domeniul cibernetic, să evite suprapunerile inutile și să asigure cooperarea și sinergiile cu inițiativele existente. Trebuie consolidate cooperarea și coordonarea între actorii din domeniul apărării cibernetice din cadrul și la nivelul UE și al statelor membre, între comunitățile cibernetice militare și civile și între ecosisteme publice și private de încredere. În acest context, statele membre sunt încurajate să exploreze și să consolideze în continuare mecanismele naționale de coordonare civil-militară, să faciliteze schimbul voluntar comun de informații, să pună la dispoziție lecțiile învățate, să contribuie la elaborarea unor standarde interoperabile și să efectueze evaluări ale riscurilor și să elaboreze scenarii de risc, precum și exerciții comune, în special la nivel european, cu respectarea deplină a dispozițiilor Directivei privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS 2).

6. Recunoscând eforturile de a spori în continuare reziliența Uniunii prin intermediul NIS 2 și al Directivei privind reziliența entităților critice (CER), Consiliul își reiterează recomandarea privind o abordare coordonată la nivelul UE pentru a consolida reziliența infrastructurii critice[1]. Acesta solicită măsuri de consolidare în continuare a rezilienței entităților critice, a infrastructurii, a produselor și serviciilor digitale, menționând, în același timp, că punerea în aplicare corespunzătoare a NIS 2 rămâne cel mai important pas. Deși este în principal o responsabilitate civilă, acest lucru contribuie, de asemenea, la o apărare cibernetică mai puternică. În acest context, IOAUE și statele membre sunt încurajate să sprijine dezvoltarea și implementarea în continuare a mecanismelor de coordonare noi și existente ale UE, a evaluărilor riscurilor, a evaluărilor și scenariilor, a schimbului voluntar comun de informații și a exercițiilor, într-un mod care să aducă valoare adăugată și să evite suprapunerile inutile cu inițiativele existente.

7. Pentru a spori în continuare încrederea, a consolida cooperarea și a facilita schimbul de informații în timp util cu privire la incidentele cibernetice semnificative și de mare amploare care afectează sistemele de apărare, Consiliul salută inițiativa de a dezvolta în continuare Conferința comandanților cibernetici ai UE, care urmează să fie organizată de fiecare președinție a Consiliului UE, cu sprijinul Agenției Europene de Apărare (AEA) și cu participarea Serviciului European de Acțiune Externă (SEAE). Consiliul încurajează toate statele membre să participe la aceste reuniuni. Pentru a consolida reziliența UE la incidentele de securitate cibernetică de mare amploare, Consiliul invită Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) și Conferința comandanților cibernetic ai UE să identifice eventuale modalități de cooperare și de valorificare a unei perspective militare și civile comune.

[1] Propunere de recomandare a Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice, COM/2022/551.

8. În vederea promovării unui răspuns mai ferm și mai coordonat la nivelul UE, Consiliul salută instituirea Rețelei operaționale a echipelor militare de răspuns la incidente de securitate informatică ale UE (MICNET)și așteaptă cu interes atingerea capabilității operaționale inițiale a acesteia până la jumătatea anului 2024, pentru a consolida schimbul de informații tehnice între statele membre participante cu privire la incidentele cibernetice care afectează sistemele de apărare. Consiliul încurajează toate statele membre să participe la MICNET pentru a asigura eficacitatea rețelei. În plus, Consiliul invită statele membre să se bazeze pe lecțiile învățate în cadrul rețelei echipelor de intervenție în caz de incidente de securitate informatică (CSIRT) și încurajează ferm crearea unui mecanism eficace de cooperare și coordonare între cele două rețele la momentul oportun, cu respectarea deplină a mecanismelor de guvernanță și a circumscripțiilor fiecărei entități.

9. Având în vedere creșterea numărului de activități cibernetice răuvoitoare ale unor actorilor statali și nestatali îndreptate împotriva misiunilor și operațiilor PSAC ale UE, Consiliul invită UE și statele sale membre să-și consolideze capabilitățile de apărare și securizare a misiunilor și operațiilor PSAC. În acest sens, Consiliul salută obiectivele de a promova în continuare protecția rețelelor și a structurilor militare ale UE, în concordanță, printre altele, cu Viziunea și strategia militară a UE privind spațiul cibernetic ca domeniu de operații[2].

[2] EEAS(2021) 706 REV 4.

10. Consiliul reiterează concluziile Consiliului din mai 2022[3] și necesitatea de a investi în asistența noastră reciprocă în temeiul articolului 42 alineatul (7) din TUE, precum și clauza de solidaritate în temeiul articolului 222 din TFUE. Consiliul subliniază importanța aprofundării în continuare a înțelegerii comune între UE și statele sale membre cu privire la punerea în aplicare a articolului 42 alineatul (7), inclusiv în scenarii complexe care presupun un atac cibernetic, în conformitate cu principiile relevante ale dreptului internațional. Acesta salută posibilitatea de a beneficia de sprijin din partea UE, la cererea explicită a statului membru (statelor membre) în cauză, atunci când se produce un atac cibernetic, fără a aduce atingere caracterului specific al politicii de securitate și apărare a anumitor state membre.

11. Consiliul subliniază progresele înregistrate în privința proiectului PESCO „Echipe de răspuns rapid în domeniul cibernetic și asistența reciprocă în ceea ce privește securitatea cibernetică” (CRRT) și disponibilitatea sa de a acționa, la cerere, drept capabilitate pentru nevoile statelor membre și ale UE, în sprijinul misiunilor și operațiilor PSAC, și de a oferi asistență partenerilor UE. Consiliul salută dezvoltarea în continuare a capabilității proiectului PESCO CRRT, a echipelor naționale de răspuns cibernetic și, după caz, a capabilităților suplimentare de răspuns la incidente, cum ar fi viitoarele echipe de răspuns rapid în caz de amenințări hibride, astfel cum sunt prevăzute în Busola strategică, inclusiv prin promovarea coordonării și cooperării acestora la nivelul UE.

[3] Concluziile Consiliului privind dezvoltarea poziției cibernetice a Uniunii Europene, 23 mai 2022, 9364/22.

12. Consiliul salută activitatea proiectului PESCO Centrul de coordonare în domeniul cibernetic și informațional (CIDCC), care vizează furnizarea unei capabilități militare de colectare și analiză a informațiilor relevante în vederea obținerii unui tablou operațional comun în domeniul cibernetic. În plus, Consiliul salută propunerea de a integra validarea conceptului, în cazul în care acesta îndeplinește cu succes rolul de centru de coordonare a informațiilor, începând cu 2025, într-un Centru de coordonare a apărării cibernetice al UE (EUCDCC), îmbunătățind coordonarea și conștientizarea situației, în special în ceea ce privește comandanții misiunilor și operațiilor PSAC ale UE, precum și consolidând arhitectura mai amplă de comandă și control a UE. Consiliul invită Înaltul Reprezentant să prezinte un concept și o foaie de parcurs pentru instituirea EUCDCC, care să reflecte învățămintele desprinse de la entități internaționale similare, să identifice resursele necesare, să evite suprapunerile inutile și să urmărească complementaritatea cu cadrul mai larg al UE în materie de securitate cibernetică.

13. Consiliul subliniază importanța cooperării strategice în materie de informații privind amenințările și activitățile cibernetice și invită statele membre, prin intermediul autorităților lor competente, să contribuie în continuare la activitatea INTCEN UE, a Direcției pentru informații a EUMS și a statelor membre în cadrul Capacității unice de analiză a informațiilor (SIAC). În plus, Consiliul subliniază importanța consolidării capacităților noastre în materie de informații cibernetice pentru a ne consolida reziliența cibernetică și răspunsurile și pentru a oferi sprijin eficace misiunilor și operațiilor noastre civile și militare din cadrul PSAC, precum și forțelor noastre armate și capacității SIAC în domeniul cibernetic, pe baza contribuțiilor voluntare cu informații din partea statelor membre și fără a aduce atingere competențelor acestora.

14. Consiliul ia act de centrul de analiză și de cunoaștere a situației în materie cibernetică al Comisiei Europene, care urmărește să consolideze conștientizarea situației de către Comisie. Consiliul subliniază importanța stabilirii unei cooperări reciproc avantajoase între acest centru și alte IOAUE, în special ENISA și CERT-UE. Consiliul subliniază importanța asigurării unei cooperări strânse cu rețelele de cooperare ale UE atunci când dezvoltă conștientizarea situației, precum și a respectării confidențialității. Consiliul ia act de necesitatea de a consolida conștientizarea comună a situației la nivelul UE și de a dezvolta în continuare cadrul UE de gestionare a crizelor în materie de securitate cibernetică, evitând, în același timp, orice suprapunere inutilă a eforturilor.

15. Consiliul reamintește că educația, formarea și exercițiile în domeniul cibernetic sunt esențiale pentru a asigura pregătirea și eficacitatea și salută activitățile naționale și cele furnizate de UE prin intermediul Colegiului European de Securitate și Apărare (CESA), al AEA, al ENISA și al proiectelor PESCO în curs de desfășurare, cum ar fi Federațiile de medii cibernetice de simulare în scopuri de antrenament (*cyber ranges*) și Academia și centrul de inovare ale UE în domeniul cibernetic (CAIH). În vederea consolidării în continuare a acestor eforturi, Consiliul așteaptă cu interes instituirea proiectului-cadru al AEA CyDef-X pentru sincronizarea și sprijinirea exercițiilor de apărare cibernetică. Consiliul încurajează AEA să analizeze, în strânsă cooperare cu statele membre și cu SEAE, modul în care CyDef-X ar putea sprijini în continuare exerciții precum CYBER PHALANX, inclusiv în ceea ce privește asistența reciprocă în temeiul articolului 42 alineatul (7) din TUE și clauza de solidaritate în temeiul articolului 222 din TFUE, precum și cu Comisia și ENISA în ceea ce privește exercițiile civile. În plus, Consiliul încurajează utilizarea și dezvoltarea în continuare, în cadrul CyDef-X, a mediilor existente de testare și exerciții în domeniul apărării cibernetice, cum ar fi Federațiile de medii cibernetice de simulare în scopuri de antrenament (*cyber ranges*). Pentru a asigura un proces decizional agil și eficient în situații de criză cibernetică, Consiliul subliniază importanța desfășurării de exerciții periodice de simulare teoretică la nivelul decizional al statelor membre.

16. Consiliul ia notă de propunerea de act privind solidaritatea cibernetică și de intenția de a consolida capabilitățile de detectare a amenințărilor și a incidentelor de securitate cibernetică din UE și de răspuns la acestea. Consiliul subliniază că propunerile în acest domeniu pot fi eficace numai atunci când sunt aliniate la cadrele de gestionare a crizelor din statele membre și la nevoile acestora. Consiliul subliniază importanța testării infrastructurii critice în vederea identificării unor eventuale vulnerabilități, în cazul în care acest lucru este evaluat ca fiind benefic, drept competență națională, ținând seama de evaluările riscurilor la nivelul UE disponibile.

17. Consiliul ia act de propunerea Comisiei de instituire a unui mecanism de urgență în domeniul cibernetic, care ar putea sprijini disponibilitatea serviciilor de securitate cibernetică furnizate de furnizori privați de încredere pentru a acorda, la cerere, asistență statelor membre în cazul unor incidente de securitate cibernetică de mare amploare, subliniind, în același timp, necesitatea de a extinde un sector european al securității cibernetice cu sprijinul ECCC ca pilon esențial pentru ca acest mecanism să fie operațional. Consiliul subliniază rolul-cheie al fiecărui stat membru în monitorizarea și evaluarea nevoilor sale naționale.

II. **Securizarea ecosistemului de apărare al UE**

18. Consiliul reamintește că încurajează statele membre să-și dezvolte în continuare propriile capabilități de a desfășura operații de apărare cibernetică, inclusiv, după caz, măsuri proactive de apărare prin care să se protejeze de atacurile cibernetice, să le detecteze, să le descurajeze și să se apere împotriva lor. Având în vedere că NIS 2 nu se aplică entităților administrației publice care își desfășoară activitățile în domeniul apărării, Consiliul invită AEA, cu sprijinul Comisiei și al SEAE, după caz, să sprijine statele membre în elaborarea unor recomandări voluntare fără caracter juridic obligatoriu, inspirate de NIS 2, pentru a spori securitatea cibernetică în comunitatea de apărare și invită toate statele membre să se implice activ în acest efort. Aceste recomandări ar trebui să țină seama de eforturile asemănătoare depuse în alte cadre.

19. Astfel cum s-a recunoscut în Busola strategică, capacitatea UE de a acționa depinde de capacitatea sa de a-și reduce dependențele strategice în toate capabilitățile sale de apărare cibernetică și lanțurile sale de aprovizionare, precum și de dezvoltarea și stăpânirea unor tehnologii de vârf pentru apărarea cibernetică. Aceasta include consolidarea bazei industriale și tehnologice de apărare europene (EDTIB) în întreaga UE, precum și a capacității acesteia de a coopera cu parteneri care împărtășesc aceeași viziune din întreaga lume, pe bază de reciprocitate, pentru a asigura beneficii reciproce. Prin urmare, Consiliul solicită sectoarelor securității cibernetice și apărării cibernetice să coopereze îndeaproape pentru a crea sinergii cu scopul de a dezvolta și de a furniza întregul spectru de capabilități de apărare cibernetică. Consiliul invită Comisia, în strânsă colaborare cu ECCC, după caz, să sprijine în continuare dezvoltarea unei baze industriale și tehnologice de apărare cibernetică europene puternice, agile, competitive la nivel mondial și inovatoare, inclusiv a întreprinderilor mici și mijlocii (IMM-uri), prin noi investiții și acțiuni de politică.

20. Având în vedere importanța interoperabilității și a caracterului comun al capabilităților de apărare cibernetică, inclusiv în ceea ce privește dezvoltarea în colaborare a unor capabilități de apărare cibernetică de nouă generație, Consiliul invită AEA și Statul-Major al UE să lucreze la un set de cerințe ale UE privind interoperabilitatea în domeniul apărării cibernetice, care s-ar baza pe principiile, procesele și standardele existente stabilite în special în cadrul Organizației Tratatului Atlanticului de Nord (NATO) și ar fi compatibile cu acestea. În plus, Consiliul invită statele membre să analizeze, în cadrul Comitetului european de standardizare în domeniul apărării, dacă ar putea fi necesare standarde voluntare specifice pentru sistemele de apărare, în strânsă cooperare cu toate părțile interesate relevante, inclusiv cu organizațiile de standardizare europene și cu NATO, după caz.

21. Consiliul salută eforturile Comisiei de a prezenta un plan de promovare a utilizării standardelor existente pentru utilizări civile în materie de securitate cibernetică și apărare cibernetică, precum și elaborarea de noi standarde voluntare. Consiliul subliniază necesitatea alinierii standardelor de securitate cibernetică și a celor de apărare cibernetică, după caz. Consiliul recunoaște că astfel de standarde voluntare ar putea fi utile pentru industriile securității cibernetice și apărării cibernetice din UE și îndeamnă la o colaborare mai strânsă între organismele de standardizare civile și cele din domeniul apărării.

22. Consiliul solicită elaborarea rapidă a unor recomandări bazate pe inventarierea de către Comisie și instituțiile relevante a instrumentelor existente pentru comunicații securizate în domeniul cibernetic. Atunci când este posibil, recomandările ar trebui să fie aliniate la inițiativele existente privind schimbul de informații și ar trebui, de asemenea, să țină seama de riscurile pe care le prezintă tehnologiile emergente și disruptive pentru metodele actuale de criptare.

23. În plus, Consiliul salută activitatea inițială desfășurată cu privire la evaluarea riscurilor și elaborarea unor scenarii de către Comisie, Înaltul Reprezentant și Grupul de cooperare NIS în ceea ce privește, pentru început, sectoarele energiei și telecomunicațiilor, la solicitarea Consiliului. Consiliul recunoaște că sunt în curs de pregătire, de asemenea, evaluări ale riscurilor specifice în materie de securitate cibernetică pentru infrastructura și rețelele de comunicații din UE. Consiliul reiterează că o înțelegere comună a impactului posibil al incidentelor cibernetice între statele membre, dar și între instituțiile, organele și agențiile UE este extrem de importantă. Astfel, Consiliul invită actorii menționați anterior să se asigure că evaluările riscurilor, scenariile de risc și recomandările ulterioare sunt luate în considerare la definirea și stabilirea priorităților măsurilor și sprijinului, la nivelul UE și, după caz, la nivel național. În plus, Consiliul solicită ca scenariile de risc să fie luate în considerare de către toți actorii relevanți în procesele de evaluare a riscurilor, precum și în elaborarea exercițiilor cibernetice.

III. **Investiții în capabilitățile de apărare cibernetică**

24. Consiliul încurajează statele membre să-și sporească investițiile pentru a construi, a menține și a dezvolta în continuare capabilități interoperabile de apărare cibernetică. Consiliul sprijină elaborarea unui set de angajamente voluntare pentru dezvoltarea în continuare a capabilităților naționale de apărare cibernetică, ținând seama de eforturile similare depuse în alte cadre.

25. Consiliul invită statele membre și AEA să valorifice oportunitatea revizuirii planului de dezvoltare a capabilităților pentru a stabili un nivel ridicat de ambiție în ceea ce privește dezvoltarea apărării cibernetice în colaborare la nivelul UE. Mai mult, Consiliul încurajează statele membre să se bazeze pe setul actualizat de priorități și pe angajamentele lor în cadrul PESCO pentru a-și spori nivelul de implicare în proiecte în colaborare ale UE de dezvoltare a capabilităților de apărare cibernetică, recunoscând beneficiile directe ale proiectelor în colaborare la nivelul UE pentru a sprijini dezvoltarea capabilităților naționale de apărare cibernetică.

26. Consiliul salută eforturile de cercetare în colaborare la nivelul UE pentru a explora eventualele aplicații în sistemele din domeniul apărării ale tehnologiilor emergente și disruptive, luând act, de asemenea, de necesitatea de a se asigura că aceste evoluții tehnologice sunt integrate rapid în capabilitățile existente și viitoare. Consiliul încurajează statele membre și industria UE să utilizeze în mod optim oportunitățile de cercetare în colaborare la nivelul UE, de exemplu cele din cadrul AEA, proiectele PESCO în curs, precum Academia și centrul de inovare ale UE în domeniul cibernetic (CAIH), Fondul european de apărare și, dacă este relevant, Orizont Europa și Programul „Europa digitală” pentru proiecte cu dublă utilizare. În plus, Consiliul salută valorificarea cadrelor specifice pentru a sprijini inovarea în domeniul apărării utilizând proiecte de tip spin-in din domeniul civil, în special Sistemul UE de inovare în domeniul apărării și Centrul european de inovare în domeniul apărării. În plus, Consiliul încurajează Centrul european de competențe în materie de securitate cibernetică (ECCC) și AEA să elaboreze un acord de lucru pentru a facilita schimbul de informații între membrii personalului acestora în legătură cu prioritățile în privința tehnologiilor civile, cu dublă utilizare și, respectiv, de apărare, în vederea creării de sinergii și a evitării suprapunerii eforturilor.

27. Consiliul salută intenția Comisiei, în cooperare cu AEA și ECCC, în concordanță cu mandatele lor respective, cu statele membre și în consultare cu părțile interesate relevante, cum ar fi industria, de a elabora o foaie de parcurs tehnologică pentru tehnologiile cibernetice critice care, prin identificarea tehnologiilor cibernetice critice și inventarierea evoluțiilor tehnologice și a dependențelor strategice, să ofere modalități de reducere a acestora, în sprijinul autonomiei strategice și al suveranității tehnologice a UE, menținând în același timp o economie deschisă. Consiliul ia act de faptul că foaia de parcurs tehnologică pentru tehnologiile cibernetice critice poate sta la baza priorităților strategice pentru instrumentele de finanțare ale UE, fiind în același timp în concordanță cu modalitățile respective în vigoare pentru acestea. Consiliul reamintește că UE ar trebui să urmărească o politică industrială europeană ambițioasă și asertivă pentru a crea un mediu de afaceri durabil, atractiv și competitiv, care să permită, de asemenea, extinderea entităților europene din domeniul cibernetic.

28. Consiliul apreciază intenția de a elimina lacunele semnificative în materie de competențe privind securitatea cibernetică prin atragerea de noi profesioniști în domeniu, inclusiv de femei, prin perfecționare și recalificare, precum și prin investiții în formare și exerciții și prin organizarea de cursuri de formare și exerciții pentru a avea o forță de muncă diversă și incluzivă în domeniul cibernetic. Recunoscând provocările cu care se confruntă UE în ceea ce privește capitalul uman în domeniul securității cibernetice și al apărării cibernetice, Consiliul salută inițiativa Academia de competențe în materie de securitate cibernetică, care poate aduce beneficii și forței de muncă din domeniul apărării cibernetice.

29. Consiliul invită statele membre să facă schimb de informații cu privire la bune practici privind pregătirea de profesioniști calificați în domeniul securității cibernetice, valorificând sinergiile dintre inițiativele militare, civile și de asigurare a respectării legii, și solicită CESA, cu sprijinul și expertiza AEA și ENISA, să ia în considerare opțiuni de consolidare a schimbului de bune practici și de sinergii suplimentare între domeniul militar și cel civil în ceea ce privește formarea și dezvoltarea de competențe de apărare specifice domeniului cibernetic.

30. Consiliul subliniază importanța unei înțelegeri comune a componenței forței de muncă din domeniul securității cibernetice și a competențelor asociate pentru a identifica și a elimina lacunele de pe piața forței de muncă în domeniul securității cibernetice, precum și necesitatea de a implica toate părțile interesate, inclusiv statele membre și industria. Consiliul recunoaște că stabilirea unor indicatori pentru monitorizarea pieței forței de muncă în domeniul securității cibernetice ar contribui la identificarea nevoilor de competențe în materie de securitate cibernetică și la direcționarea fondurilor în mod adecvat, contribuind în același timp la îndeplinirea obligațiilor legate de politici, în special a celor care decurg din NIS 2. Consiliul salută propunerea privind un cadru de certificare a competențelor în materie de apărare cibernetică și invită Înaltul Reprezentant, în calitatea sa de șef al CESA, să dezvolte acest cadru, în cooperare cu SEAE, Comisia și statele membre, prin valorificarea inițiativelor civile.

IV. **Crearea de parteneriate pentru abordarea provocărilor comune**

31. Consiliul invită Înaltul Reprezentant și Comisia să-și consolideze și să-și promoveze cooperarea și să exploreze parteneriate reciproc avantajoase și adaptate privind politicile de apărare cibernetică, inclusiv privind consolidarea capacităților de apărare cibernetică prin intermediul Instrumentului european pentru pace (IEP). În acest scop, apărarea cibernetică ar trebui adăugată ca punct la dialogurile și consultările UE privind domeniul cibernetic și la consultările generale cu partenerii privind securitatea și apărarea. În plus, ar trebui consolidate dialogurile și colaborarea cu sectorul privat. Consiliul subliniază că o colaborare internațională privind standardele și certificarea în domeniul securității cibernetice ar reprezenta o valoare adăugată pentru industria europeană. Prin urmare, salută angajamentul Comisiei de a o trata drept componentă esențială a dialogurilor UE în domeniul cibernetic cu țări terțe și organizații internaționale.

32. Consiliul subliniază importanța cooperării internaționale pentru prevenirea sau reducerea riscurilor de conflicte în spațiul cibernetic, în special prin dezvoltarea și operaționalizarea în continuare a măsurilor de consolidare a încrederii la nivel regional și internațional, inclusiv în cadrul ONU, și prin încurajarea în continuare a utilizării măsurilor existente de consolidare a încrederii în domeniul cibernetic, cum ar fi în cadrul Organizației pentru Securitate și Cooperare în Europa (OSCE), inclusiv în perioade de tensiuni internaționale.
UE și statele sale membre subliniază că dreptul internațional existent se aplică în spațiul cibernetic și subliniază importanța unor eforturi continue de a susține și promova cadrul ONU pentru un comportament responsabil al statelor și de a întreprinde acțiuni în vederea punerii în aplicare a acestuia, inclusiv prin instituirea Programului de acțiune pentru promovarea unui comportament responsabil al statelor în spațiul cibernetic.

33. În concordanță cu declarațiile comune privind cooperarea UE-NATO, Consiliul invită Înaltul Reprezentant, inclusiv în calitatea sa de șef al AEA, precum și Comisia, să continue să consolideze, să aprofundeze și să extindă parteneriatul cu NATO în domeniul cibernetic, cu respectarea deplină a principiilor incluziunii, reciprocității, deschiderii reciproce și transparenței, precum și a autonomiei decizionale a ambelor organizații. Ținând seama de necesitatea de a asigura eforturi complementare și coordonate cu implicarea cât mai mare posibilă a statelor membre care nu fac parte din NATO și de a evita suprapunerile inutile, Consiliul solicită totodată stabilirea de legături la nivelurile relevante între UE și NATO în ceea ce privește formarea, educația, conștientizarea situației, exercițiile și platformele de C&D și identificarea unor potențiale sinergii între angajamentele voluntare respective pentru dezvoltarea capabilităților naționale de apărare cibernetică și a cadrelor de gestionare a crizelor, protecția infrastructurii critice și consolidarea schimburilor în materie de conștientizare a situației, a răspunsurilor coordonate la activitățile cibernetice răuvoitoare, precum și a eforturilor de consolidare a capacităților în țările terțe. Printre acestea se numără acordul tehnic dintre Capacitatea de răspuns la incidente informatice (NCIRC) din cadrul NATO și Centrul de răspuns la incidente de securitate cibernetică al UE (CERT-UE), precum și un dialog politic consolidat privind aspectele legate de apărarea cibernetică la toate nivelurile.

V. **Concluzie**

34. Luând ca bază Concluziile Consiliului privind politica UE în domeniul apărării cibernetice, Consiliul invită Înaltul Reprezentant și Comisia să elaboreze, în vederea aprobării de către statele membre, un plan de punere în aplicare a acestei politici până în al doilea trimestru al anului 2023. De asemenea, Consiliul invită statele membre să-și declare în mod voluntar ambițiile și acțiunile în ceea ce privește apărarea cibernetică în contextul politicii UE în domeniul apărării cibernetice și să utilizeze pe deplin recomandările și angajamentele voluntare fără caracter juridic obligatoriu pentru a-și intensifica eforturile de apărare cibernetică la nivel național și multinațional, cu scopul de a maximiza impactul la nivelul UE. Înaltul Reprezentant, Comisia și statele membre sunt invitate să raporteze și să discute anual în legătură cu progresele înregistrate în ceea ce privește punerea în aplicare a elementelor comunicării comune și a planului de punere în aplicare a acesteia începând cu al doilea trimestru al anului 2024.