Consiliul
Uniunii Europene

Bruxelles, 23 mai 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	23 mai 2022
Destinatar:	Delegațiile
Subiect:	Concluzii ale Consiliului privind dezvoltarea poziției cibernetice a Uniunii Europene - Concluziile Consiliului aprobate de Consiliu în cadrul reuniunii sale din 23 mai 2022

În anexă, se pun la dispoziția delegațiilor Concluziile Consiliului privind dezvoltarea poziției cibernetice a Uniunii Europene, astfel cum au fost aprobate de Consiliu în cadrul reuniunii sale din 23 mai 2022.

ANEXĂ

Concluziile Consiliului privind dezvoltarea poziției cibernetice a Uniunii Europene

CONSILIUL UNIUNII EUROPENE,

REAMINTIND concluziile sale privind:

– Comunicarea comună din 25 iunie 2013 către Parlamentul European și Consiliu privind Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat[1],

– un cadru politic de apărare cibernetică al UE[2],

– guvernanța internetului[3],

– diplomația cibernetică[4],

– consolidarea sistemului de reziliență cibernetică al Europei și promovarea unui sector al securității cibernetice competitiv și inovator[5]

– Comunicarea comună din 20 noiembrie 2017 către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”[6],

– un cadru privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare („Setul de instrumente pentru diplomația cibernetică”)[7],

– răspunsul coordonat al UE la incidentele și crizele de securitate cibernetică de mare amploare[8],

– Orientările privind consolidarea capacităților cibernetice externe ale UE[9],

---

1 12109/13.
2 15585/14.
3 16200/14.
4 6122/15 + COR 1.
5 14540/16.
6 14435/17 + COR 1.
7 10474/17.
8 10086/18.
9 10496/18.

– Decizia de punere în aplicare (UE) 2018/1993 a Consiliului din 11 decembrie 2018 privind mecanismul integrat al Uniunii pentru un răspuns politic la crize[10],

– consolidarea capacităților și a capabilităților în domeniul securității cibernetice în UE[11],

– importanța tehnologiei 5G pentru economia europeană și necesitatea de a atenua riscurile pentru securitate legate de tehnologia 5G[12],

– viitorul unei Europe cu un grad ridicat de digitalizare după 2020: „Stimularea competitivității digitale și economice în întreaga Uniune și a coeziunii digitale”[13],

– eforturi complementare de sporire a rezilienței și de contracarare a amenințărilor hibride[14],

– conturarea viitorului digital al Europei[15],

– securitatea cibernetică a dispozitivelor conectate[16],

– Strategia de securitate cibernetică a UE pentru deceniul digital[17],

– securitatea și apărarea[18],

– explorarea potențialului inițiativei privind unitatea cibernetică comună, în completarea răspunsului coordonat al UE la incidentele și crizele de securitate cibernetică de mare amploare[19],

– 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[20],

---

10 JO L 320, 17.12.2018, p. 28-34.
11 7737/19.
12 14517/19.
13 9596/19.
14 14972/19.
15 8711/20.
16 13629/20.
17 7290/21.
18 8396/21.
19 13048/21.
20 7371/22.

1. SUBLINIAZĂ că în ultimii ani s-au intensificat comportamentele răuvoitoare în spațiul cibernetic, atât din partea unor actori statali, cât și din partea unor actori nestatali, înregistrându-se o creștere puternică și constantă a activităților răuvoitoare care vizează infrastructura critică, lanțurile de aprovizionare și proprietatea intelectuală ale UE și ale statelor sale membre, un risc sporit de propagare, precum și o creștere a atacurilor de tip *ransomware* împotriva întreprinderilor, a organizațiilor și a cetățenilor noștri. CONSTATĂ că, odată cu revenirea la politica raporturilor de forță, unele țări încearcă din ce în ce mai mult să conteste și să submineze ordinea internațională bazată pe norme în spațiul cibernetic, transformând sfera cibernetică, alături de marea liberă, spațiul aerian și spațiul cosmic, într-un domeniu din ce în ce mai contestat. RECUNOAȘTE că atacurile cibernetice de mare amploare sau tentativele de intruziune, perturbare sau distrugere a rețelelor și sistemelor informatice care provoacă efecte sistemice au devenit mai frecvente, ar putea submina securitatea noastră economică și ne-ar putea afecta instituțiile și procesele democratice și arată că unii actori sunt dispuși să pună în pericol securitatea și stabilitatea internaționale. SUBLINIAZĂ că agresiunea militară a Rusiei împotriva Ucrainei a demonstrat că pot fi desfășurate activități cibernetice ofensive ca parte integrantă a strategiilor hibride care combină intimidarea, destabilizarea și perturbarea economică.

2. REITEREAZĂ că, în contextul schimbărilor geopolitice actuale, forța Uniunii noastre constă în unitate, solidaritate și hotărâre și că punerea în aplicare a Busolei strategice va consolida autonomia strategică a UE și capacitatea sa de a colabora cu partenerii pentru a-și proteja valorile și interesele, inclusiv în domeniul cibernetic. SUBLINIAZĂ că o UE mai puternică și mai capabilă în materie de securitate și apărare va aduce o contribuție pozitivă la securitatea mondială și transatlantică și este complementară NATO, care rămâne baza apărării colective pentru membrii săi. REAFIRMĂ intenția UE de a intensifica sprijinul pentru ordinea internațională bazată pe norme, în centrul căreia se află Organizația Națiunilor Unite.

3. În conformitate cu Concluziile Consiliului privind Strategia de securitate cibernetică a UE și cu Busola strategică, REITEREAZĂ necesitatea de a dezvolta poziția cibernetică a Uniunii consolidând capacitatea noastră de a preveni atacurile cibernetice prin consolidarea capacităților, dezvoltarea capabilităților, formare, exerciții, precum și printr-o reziliență sporită și printr-un răspuns ferm la atacurile cibernetice împotriva UE și a statelor sale membre utilizând toate instrumentele UE disponibile. Aceasta include a demonstra în continuare hotărârea UE de a oferi răspunsuri imediate și pe termen lung actorilor care generează amenințări și care urmăresc să împiedice accesul nostru sigur și deschis la spațiul cibernetic și să prejudicieze interesele noastre strategice, inclusiv securitatea partenerilor noștri. În acest context, SUBLINIAZĂ că poziția cibernetică urmărește să combine diferitele inițiative care sprijină acțiunile UE de consolidare a păcii și a stabilității în spațiul cibernetic și în favoarea unui spațiu cibernetic deschis, liber, global, stabil și sigur, concomitent cu o mai bună coordonare a acțiunilor pe termen scurt, mediu și lung de prevenire, descurajare și răspuns la amenințările și atacurile cibernetice și cu o mobilizare a capabilităților cibernetice. SUBLINIAZĂ că aceste elemente ar trebui incluse în poziția cibernetică a UE, în conformitate cu cinci funcții ale UE în domeniul cibernetic: consolidarea rezilienței noastre cibernetice și a capacităților noastre de protecție; consolidarea gestionării solidare și cuprinzătoare a crizelor; promovarea viziunii noastre asupra spațiului cibernetic; consolidarea cooperării cu țări partenere și cu organizații internaționale; prevenirea atacurilor cibernetice, apărarea împotriva acestora și răspunsul la acestea.

I. CONSOLIDAREA REZILIENȚEI NOASTRE CIBERNETICE ȘI A CAPACITĂȚILOR NOASTRE DE PROTECȚIE

4. REITEREAZĂ necesitatea de a spori nivelul global de securitate cibernetică a UE, AȘTEAPTĂ CU INTERES adoptarea rapidă a proiectului de directivă privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune (NIS 2), a proiectului de regulament privind reziliența operațională digitală a sectorului financiar (DORA), a proiectului de directivă privind reziliența entităților critice (CER) și IA ACT de propunerea de regulament privind măsuri pentru un nivel ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii, pentru a promova o Uniune Europeană care își protejează cetățenii, serviciile publice și întreprinderile în spațiul cibernetic. ÎNCURAJEAZĂ Comisia să finalizeze adoptarea unor propuneri-cheie care urmăresc să asigure că infrastructurile, tehnologiile, produsele și serviciile digitale sunt securizate, pentru a transmite un semnal clar cu privire la ambițiile UE în aceste domenii și pentru a permite sprijinirea întreprinderilor astfel încât să facă față provocării. INVITĂ Comisia să propună cerințe comune la nivelul UE în materie de securitate cibernetică pentru dispozitivele conectate și procesele și serviciile asociate prin intermediul Actului privind reziliența cibernetică, care ar trebui să fie propus de Comisie înainte de sfârșitul anului 2022, ținând seama de necesitatea unei abordări orizontale și globale care să cuprindă întregul ciclu de viață al produselor și serviciilor digitale, precum și de reglementările existente, în special în domeniul securității cibernetice.

5. INVITĂ autoritățile relevante, cum ar fi Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC), Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) și Grupul de cooperare pentru securitatea rețelelor și a informațiilor (NIS), împreună cu Comisia Europeană, să formuleze recomandări, pe baza unei evaluări a riscurilor, adresate statelor membre și Comisiei Europene pentru a consolida reziliența rețelelor și infrastructurilor de comunicații în cadrul Uniunii Europene, inclusiv continuarea punerii în aplicare a setului de instrumente al UE pentru 5G.

6. INVITĂ UE și statele sale membre să își intensifice eforturile vizând creșterea nivelului general de securitate cibernetică, de exemplu prin facilitarea apariției unor furnizori de servicii de securitate cibernetică de încredere, și SUBLINIAZĂ că încurajarea dezvoltării unor astfel de furnizori ar trebui să fie o prioritate pentru politica industrială a UE în domeniul securității cibernetice. Pentru a rezista mai bine atacurilor cibernetice cu potențiale efecte sistemice și a contracara astfel de atacuri și pe baza lecțiilor desprinse din gestionarea vulnerabilităților Solarwinds, Microsoft Exchange și Apache Log4J, INVITĂ Comisia să propună opțiuni pentru a încuraja apariția unei industrii a serviciilor de securitate cibernetică de încredere, pentru a consolida securitatea cibernetică a lanțului de aprovizionare TIC, pentru a aborda efectele potențiale ale vulnerabilităților programelor informatice pentru UE și statele sale membre, inclusiv în perspectiva viitorului Act privind reziliența cibernetică și pentru a îmbunătăți capabilitățile de detectare a amenințărilor cibernetice și de partajare a acestora în statele membre și între acestea.

7. REITERÂND faptul că investițiile în inovare și o mai bună utilizare a tehnologiei civile sunt esențiale pentru consolidarea suveranității noastre tehnologice, inclusiv în domeniul cibernetic, SOLICITĂ Comisiei să opereționalizeze rapid Centrul european de competențe în materie de securitate cibernetică pentru a dezvolta un ecosistem european solid de cercetare, industrie și tehnologie în domeniul cibernetic, SUBLINIAZĂ necesitatea de a stimula cercetarea și inovarea, de a investi mai mult în domeniile civil și de apărare pentru a consolida baza industrială și tehnologică de apărare (EDTIB) a UE și de a dezvolta capabilitățile cibernetice ale UE și ale statelor sale membre, inclusiv capacitățile de sprijin strategic. SUBLINIAZĂ importanța utilizării intensive a noilor tehnologii, în special informatica cuantică, inteligența artificială și *Big Data*, pentru a obține avantaje comparative, inclusiv în ceea ce privește operațiunile de răspuns la incidente cibernetice.

8. RECUNOSCÂND că îmbunătățirea securității noastre cibernetice este o modalitate de a spori eficacitatea și securitatea eforturilor noastre pe uscat, în spațiul aerian, pe mare și în spațiul cosmic, SUBLINIAZĂ importanța integrării considerentelor de securitate cibernetică în toate politicile publice ale UE, inclusiv în legislația sectorială în complementaritate cu Directiva NIS 2, și INVITĂ Comisia să analizeze opțiunile de creștere a securității cibernetice de-a lungul întregului lanț de aprovizionare al bazei industriale și tehnologice de apărare (EDTIB) a UE.

9. RECUNOAȘTE că asigurarea unor resurse financiare și umane adecvate pentru securitatea cibernetică și măsurile care vizează crearea unui mediu favorabil pentru competitivitatea sectorului privat sunt esențiale pentru dezvoltarea poziției cibernetice a UE și că chestiunea finanțării stabile și pe termen lung a securității cibernetice ar trebui, de asemenea, abordată la nivelul UE prin conceperea și punerea în aplicare a unui mecanism orizontal care să combine mai multe surse de finanțare, inclusiv costul aferent resurselor umane cu înaltă calificare. Prin urmare, SOLICITĂ Comisiei să analizeze opțiunile pentru un astfel de mecanism înainte de sfârșitul anului 2022, urmând a fi discutate în cadrul organismelor relevante ale Consiliului.

10. SUBLINIAZĂ necesitatea de a ne consolida eforturile și de a ne intensifica cooperarea în lupta împotriva criminalității informatice internaționale, în special de tip *ransomware*, prin intermediul mecanismului EMPACT (Platforma multidisciplinară europeană împotriva amenințărilor infracționale), prin schimburi între sectorul securității cibernetice, sectorul asigurării respectării legii și sectorul diplomatic, precum și prin consolidarea capabilităților în materie de asigurare a respectării legii în ceea ce privește investigarea și urmărirea penală a criminalității informatice. ÎȘI REITEREAZĂ angajamentul de a informa publicul cu privire la amenințările cibernetice și la măsurile luate la nivel național și la nivelul UE împotriva acestor amenințări, prin implicarea societății civile, a sectorului privat și a mediului academic, în vederea sensibilizării publicului și a încurajării unui nivel adecvat de protecție cibernetică și de igienă cibernetică. SUBLINIAZĂ necesitatea de a pune accentul pe competențele și capabilitățile de securitate cibernetică ale cetățenilor la nivelul UE și al statelor membre, precum și necesitatea de a implica activ utilizatorii în propria lor protecție.

II. **CONSOLIDAREA GESTIONĂRII SOLIDARE ȘI CUPRINZĂTOARE A CRIZELOR**

11. Pe baza exercițiilor cibernetice anuale, a altor exerciții care implică o dimensiune cibernetică și a exercițiului EU CyCLES din 2022, SUBLINIAZĂ importanța instituirii unui program de exerciții cibernetice intercomunitare și pe mai multe niveluri, desfășurate periodic, pentru a testa și a dezvolta răspunsul intern și extern al UE la incidentele cibernetice de mare amploare, cu participarea Consiliului, a SEAE, a Comisiei și a părților interesate relevante, cum ar fi ENISA și sectorul privat, care va fi articulat și va contribui la politica generală în materie de exerciții a UE. SUBLINIAZĂ importanța dezvoltării în continuare a exercițiilor Cyber Europe și BlueOLEx, combinând răspunsurile la diferite niveluri. RECUNOAȘTE necesitatea de a evalua și de a consolida exercițiile existente și de a explora posibilitatea unor exerciții suplimentare în segmente specifice ale domeniului cibernetic, în special un exercițiu CERT în domeniul militar și un exercițiu axat pe cooperarea în situații de criză între EUIBA. RECUNOAȘTE că poziția cibernetică a Uniunii ne va consolida capacitatea de prevenire a atacurilor cibernetice prin diverse acțiuni, inclusiv prin formare, și, prin urmare, INVITĂ statele membre să consolideze cooperarea civilo-militară în domeniul formării cibernetice și al exercițiilor comune.

12. SUBLINIAZĂ necesitatea de a testa și consolida în continuare cooperarea operațională și conștientizarea comună a situației în rândul statelor membre, inclusiv prin intermediul unor rețele consacrate, cum ar fi rețeaua CSIRT și Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (CyCLONe UE), pentru a realiza progrese în privința nivelului de pregătire a UE pentru a face față incidentelor cibernetice de mare amploare. SUBLINIAZĂ că este important să se lucreze la elaborarea unui limbaj comun între statele membre și cu EUIBA, care să fie adaptat discuțiilor la nivel politic, pentru a sprijini stabilirea unei evaluări consolidate a gravității și a impactului incidentelor cibernetice relevante, precum și a scenariilor evoluțiilor posibile și a nevoilor care decurg din acestea, după caz. SUBLINIAZĂ, în acest sens, necesitatea de a îmbunătăți complementaritatea rapoartelor comune de evaluare a situației, inclusiv a rapoartelor CyCLONe UE privind impactul și gravitatea incidentelor cibernetice de mare amploare în statele membre ale UE și a evaluărilor amenințărilor furnizate de INTCEN UE în cadrul setului de instrumente al UE pentru diplomația cibernetică. INVITĂ Comisia, Înaltul Reprezentant și Grupul de cooperare NIS, în coordonare cu organismele și agențiile civile și militare relevante și cu rețelele consacrate, inclusiv CyCLONe UE, să realizeze, până la sfârșitul anului 2022, o evaluare a riscurilor și să elaboreze scenarii de risc din perspectiva securității cibernetice într-o situație de amenințare sau de posibil atac împotriva statelor membre sau a țărilor partenere și să le prezinte organismelor relevante ale Consiliului. SUBLINIAZĂ necesitatea unei comunicări publice adecvate și coordonate cu privire la răspunsul UE la incidentele cibernetice de mare amploare.

13. În cazul unui incident cibernetic de mare amploare, SUBLINIAZĂ necesitatea de a consolida coordonarea și, după caz, valorificând progresele înregistrate și activitatea desfășurată de echipele de răspuns rapid în domeniul cibernetic din cadrul PESCO și pornind de la activitatea rețelei CSIRT și a CyCLONe UE, punerea în comun voluntară a capacităților noastre de răspuns la incidente între statele membre. RECUNOAȘTE că dezvoltarea legăturilor cu sectorul privat ar putea fi un amplificator al capacităților publice, în special în contextul lipsei de personal calificat în întreaga UE, și că identificarea și coordonarea acestor parteneri privați ar putea avea un impact semnificativ în cazul unor incidente de mare amploare. În vederea asigurării unei pregătiri depline pentru a face față incidentelor cibernetice de mare amploare, INVITĂ Comisia să prezinte o propunere privind un nou Fond de răspuns la situații de urgență legate de securitatea cibernetică până la sfârșitul celui de al treilea trimestru al anului 2022.

14. În concordanță cu Busola strategică, REITEREAZĂ necesitatea de a investi în asistența noastră reciprocă, în temeiul articolului 42 alineatul (7) din Tratatul privind Uniunea Europeană, precum și în solidaritate, în temeiul articolului 222 din Tratatul privind funcționarea Uniunii Europene, în special prin exerciții frecvente. În acest cadru, SUBLINIAZĂ necesitatea continuării lucrărilor cu privire la furnizarea și coordonarea sprijinului civil și/sau militar bilateral, inclusiv prin explorarea posibilității oferirii de sprijin din partea UE la cererea explicită a statelor membre, precum și cu privire la identificarea unor măsuri de răspuns adecvate, inclusiv prin dezvoltarea unei strategii de comunicare coordonate, în contextul punerii în aplicare a articolului 42 alineatul (7). IA ACT de faptul că aceasta ar trebui să includă, de asemenea, analizarea legăturilor cu mecanismele existente ale UE de gestionare a crizelor și cu mecanismul de protecție civilă al UE.

15. SUBLINIAZĂ că o poziție cibernetică consolidată a UE va presupune îmbunătățirea comunicațiilor securizate. În acest scop, REITEREAZĂ orientările oferite de Busola strategică în această privință și INVITĂ Comisia și alte instituții, organe și agenții relevante să desfășoare, până la sfârșitul anului 2022, o cartografiere a instrumentelor existente pentru comunicații securizate în domeniul cibernetic care urmează să fie discutată în cadrul organismelor relevante ale Consiliului și cu grupurile de cooperare relevante, cum ar fi rețeaua CSIRT și CyCLONe UE.

III. PROMOVAREA VIZIUNII NOASTRE ASUPRA SPAȚIULUI CIBERNETIC

16. REAMINTEȘTE că abordarea comună și cuprinzătoare a UE în ceea ce privește diplomația cibernetică urmărește să contribuie la prevenirea conflictelor, la atenuarea amenințărilor la adresa securității cibernetice și la o mai mare stabilitate în relațiile internaționale. În acest context, REAFIRMĂ angajamentul UE față de soluționarea litigiilor internaționale în spațiul cibernetic prin mijloace pașnice și aplicarea dreptului internațional, inclusiv a dreptului internațional al drepturilor omului și a dreptului internațional umanitar, în cazul acțiunilor statelor în spațiul cibernetic. SUBLINIAZĂ angajamentul UE și al statelor sale membre de a acționa în conformitate cu normele voluntare și neobligatorii privind comportamentul responsabil al statelor în spațiul cibernetic, convenite de toate statele membre ale ONU. SUBLINIAZĂ importanța unui spațiu cibernetic deschis, liber, global, stabil și sigur, în care drepturile omului, libertățile fundamentale și statul de drept să se aplice pe deplin, în sprijinul bunăstării sociale, al creșterii economice, al prosperității și integrității societăților noastre libere și democratice și REAFIRMĂ angajamentul UE și al statelor sale membre de a continua promovarea acestor valori și principii. În vederea dezvoltării unor canale pentru un dialog constructiv, sincer și deschis cu principalele părți interesate din spațiul cibernetic, SUBLINIAZĂ importanța transformării aspectelor cibernetice, inclusiv a setului de instrumente al UE pentru diplomația cibernetică, într-o parte integrantă a negocierilor de aderare la Uniune și a dialogurilor strategice și politice ale UE cu parteneri internaționali și cu concurenți deopotrivă și, în același timp, SOLICITĂ Înaltului Reprezentant să revizuiască dialogurile cibernetice bilaterale existente și, dacă este necesar, să propună inițierea unei cooperări similare cu alte țări sau cu organizații internaționale relevante.

17. REAMINTEȘTE importanța cooperării cu mai multe părți interesate, întrucât și alte părți interesate sunt responsabile pentru securitatea cibernetică, în special în ceea ce privește punerea în aplicare a recomandărilor și a deciziilor luate în cadrul forurilor internaționale și regionale. INVITĂ UE și statele sale membre să promoveze în continuare modelul nostru de spațiu cibernetic și de internet pe baza abordării care implică mai multe părți interesate și prin intermediul unor inițiative precum Apelul de la Paris la încredere și securitate în spațiul cibernetic și Declarația privind viitorul internetului, subliniind beneficiile comune ale stabilității în spațiul cibernetic și crescând gradul de conștientizare la nivel mondial cu privire la pericolele unei viziuni etatiste și autoritare asupra internetului și INVITĂ UE și statele sale membre să consolideze în continuare cooperarea cu comunitatea care cuprinde mai multe părți interesate, inclusiv prin recurgerea la proiecte relevante cum ar fi Inițiativa pentru diplomația cibernetică a UE din cadrul Instrumentului de politică externă al UE.

18. SE ANGAJEAZĂ să se implice permanent în organizațiile internaționale relevante, în special în procesele legate de Comisia I și Comisia III a ONU, subliniind, în același timp, că dreptul internațional existent se aplică, fără rezerve, în spațiul cibernetic și în ceea ce privește spațiul cibernetic. SUBLINIAZĂ importanța continuării eforturilor de susținere și promovare a cadrului ONU pentru un comportament responsabil al statelor și SUBLINIAZĂ că UE și statele sale membre vor acționa în mod activ în direcția consolidării punerii sale în aplicare, inclusiv prin instituirea Programului de acțiune pentru promovarea unui comportament responsabil al statelor în spațiul cibernetic. SUBLINIAZĂ că UE și statele sale membre se vor implica activ în negocierile pentru o viitoare Convenție a ONU care să servească drept instrument eficace pentru autoritățile de aplicare a legii și autoritățile judiciare în lupta mondială împotriva criminalității informatice, luând în considerare pe deplin cadrul existent al instrumentelor internaționale și regionale în acest domeniu, în special Convenția de la Budapesta privind criminalitatea informatică. SUBLINIAZĂ importanța sprijinirii în continuare a dezvoltării și a operaționalizării măsurilor de consolidare a încrederii (CBM) la nivel regional și internațional și a încurajării în continuare a utilizării CBM cibernetice existente în cadrul OSCE, inclusiv în perioade marcate de tensiuni internaționale.

19. REAMINTEȘTE că o abordare proactivă, bazată pe drepturile omului în ceea ce privește respectarea standardelor internaționale în domeniile tehnologiilor emergente și arhitecturii de bază a internetului în concordanță cu valorile și principiile democratice este esențială pentru a asigura că internetul rămâne global, nefragmentat și deschis și SPRIJINĂ principiul utilizării și dezvoltării tehnologiilor într-un mod care respectă drepturile omului și protejează viața privată și utilizarea lor legală, sigură și etică. ÎNCURAJEAZĂ Înaltul Reprezentant și Comisia să elaboreze o viziune strategică asupra aspectelor tehnice din domeniul digital care au implicații de politică externă și care ar putea avea un impact asupra stabilității spațiului cibernetic și, în special, a internetului, inclusiv în cadrul organizațiilor internaționale specializate relevante (Uniunea Internațională a Telecomunicațiilor etc.).

IV. CONSOLIDAREA COOPERĂRII CU ȚĂRI PARTENERE ȘI CU ORGANIZAȚII INTERNAȚIONALE

20. SUBLINIAZĂ necesitatea de a conecta mai bine strategia UE de consolidare a capacităților cibernetice cu normele ONU privind comportamentul responsabil al statelor în spațiul cibernetic, inclusiv prin dezvoltarea unor programe de cooperare și de consolidare a capacităților adaptate pentru a sprijini statele terțe în eforturile lor de punere în aplicare și, în acest sens, prin continuarea și extinderea eforturilor noastre în sprijinul Programului de acțiune al ONU pentru promovarea unui comportament responsabil al statelor în spațiul cibernetic. SUBLINIAZĂ importanța integrării depline a consolidării capacităților cibernetice ca parte a ofertei UE în calitate de furnizor de securitate, cu o coordonare adecvată a eforturilor între statele membre și instituțiile, organele și agențiile UE și, în special, SALUTĂ cooperarea dintre statele membre, precum și cu partenerii din sectorul public și privat, în special prin intermediul rețelei CyberNet a UE (Rețeaua UE de consolidare a capacităților cibernetice) și al Forumului mondial privind competențele cibernetice (GFCE), pentru a asigura coordonarea și a evita suprapunerile.

INVITĂ Înaltul Reprezentant și Comisia să instituie un *Comitet pentru consolidarea capacităților cibernetice* până în al treilea trimestru al anului 2022 și să organizeze schimburi periodice în cadrul Grupului de lucru orizontal pentru chestiuni cibernetice. INVITĂ Comisia și Înaltul Reprezentant să mobilizeze în continuare Instrumentul de vecinătate, cooperare pentru dezvoltare și cooperare internațională (IVCDCI), Instrumentul de asistență pentru preaderare (IPA III) și alte instrumente financiare, cum ar fi Instrumentul european pentru

pace (IEP) și Inițiativa „Global Gateway”, pentru a sprijini consolidarea rezilienței partenerilor noștri, a capacității acestora de a identifica și aborda amenințările cibernetice și de a investiga și urmări penal infracțiunile informatice, precum și dezvoltarea de proiecte de cooperare, inclusiv în contextul crizelor, în special, ÎNCURAJEAZĂ cooperarea cu partenerii din Balcanii de Vest și din vecinătatea estică și sudică a UE, precum și desfășurarea de experți ai UE și ai statelor membre pentru a oferi sprijin în cazul unor crize cibernetice, luând în considerare mandatele legale existente.

21. SUBLINIAZĂ necesitatea de a intensifica eforturile în vederea elaborării unei abordări de comunicare structurate și deschise a UE în ceea ce privește modalitățile de promovare a unei înțelegeri comune la nivel mondial a aplicării dreptului internațional în spațiul cibernetic, a cadrului ONU privind comportamentul responsabil al statelor în spațiul cibernetic, inclusiv a inițiativei privind un program de acțiune pentru promovarea unui comportament responsabil al statelor în spațiul cibernetic, precum și a poziției UE și a statelor sale membre în cadrul negocierilor în curs cu privire la o Convenție a ONU privind criminalitatea informatică și, în cadrul acestor eforturi, SOLICITĂ Înaltului Reprezentant să prezinte Consiliului un plan de comunicare până la sfârșitul anului 2022. ÎNCURAJEAZĂ Înaltul Reprezentant și serviciile Comisiei să recurgă pe deplin și în mod sistematic la cele 145 de delegații și să dezvolte o colaborare regulată și fructuoasă între acestea și ambasadele statelor membre din țările terțe, sub auspiciile viitoarei rețele a diplomației cibernetice a UE. INVITĂ Înaltul Reprezentant să înființeze Rețeaua diplomației cibernetice a UE până în al treilea trimestru al anului 2022, contribuind la schimbul de informații, la activități comune de formare pentru personalul UE și al statelor membre, la eforturi coerente de consolidare a capacităților și la consolidarea punerii în aplicare a cadrului ONU pentru un comportament responsabil al statelor, precum și la măsuri de consolidare a încrederii între state.

22. SUBLINIAZĂ angajamentul său de a coopera în continuare cu organizațiile internaționale și cu țările partenere pentru a promova înțelegerea comună a peisajului amenințărilor cibernetice, pentru a dezvolta mecanisme de cooperare și pentru a identifica în mod proactiv răspunsuri diplomatice prin cooperare. AMINTIND principalele realizări ale cooperării UE-NATO în domeniul securității cibernetice în cadrul punerii în aplicare a declarațiilor comune de la Varșovia din 2016 și de la Bruxelles din 2018, cu respectarea deplină a autonomiei decizionale și a procedurilor ambelor organizații și pe baza principiilor transparenței, reciprocității și incluziunii, SUBLINIAZĂ necesitatea de a consolida în continuare cooperarea cibernetică cu NATO prin exerciții, schimb de informații și schimburi între experți, inclusiv în ceea ce privește dezvoltarea capabilităților, consolidarea capacităților pentru parteneri, misiuni și operații, precum și în ceea ce privește aplicabilitatea dreptului internațional și a normelor ONU privind un comportament responsabil al statelor în spațiul cibernetic, precum și posibilele răspunsuri coordonate la activitățile cibernetice răuvoitoare.

V. PREVENIREA ATACURILOR CIBERNETICE, APĂRAREA ÎMPOTRIVA ACESTORA ȘI RĂSPUNSUL LA ACESTEA

23. RECUNOAȘTE că spațiul cibernetic a devenit o arenă a concurenței geopolitice și, prin urmare, REITEREAZĂ că UE trebuie să fie în măsură să răspundă rapid și cu fermitate la atacurile cibernetice, cum ar fi activitățile cibernetice răuvoitoare sprijinite de stat care vizează UE și statele sale membre și, în consecință, trebuie să consolideze setul de instrumente al UE pentru diplomația cibernetică și să utilizeze pe deplin toate instrumentele sale, inclusiv instrumentele politice, economice, diplomatice, juridice și de comunicare strategică disponibile pentru a preveni, descuraja și răspunde la activitățile cibernetice răuvoitoare. SUBLINIAZĂ că actorii ostili trebuie să fie conștienți de faptul că atacurile cibernetice împotriva statelor membre și a instituțiilor UE vor fi detectate din timp, vor fi identificate prompt și li se vor aplica toate instrumentele și politicile necesare. Bazându-se în special pe elementele poziției cibernetice din cadrul acestora și pe lecțiile învățate din punerea în aplicare a setului de instrumente pentru diplomația cibernetică de la crearea sa și din exercițiul EU CyCLES, INVITĂ statele membre și Înaltul Reprezentant, cu sprijinul Comisiei, să depună eforturi în vederea elaborării, până la sfârșitul primului trimestru al anului 2023, a unei versiuni revizuite a orientărilor de punere în aplicare a setului de instrumente al UE pentru diplomația cibernetică, în special prin explorarea unor măsuri de răspuns suplimentare.

24. SUBLINIAZĂ necesitatea de a desfășura schimburi periodice cu privire la peisajul amenințărilor cibernetice în cadrul organismelor și comitetelor relevante ale Consiliului, colaborând totodată în mod regulat cu sectorul privat și bazându-se pe evaluarea impactului și gravității incidentelor recente, pentru a spori gradul general de conștientizare și de pregătire pentru aplicarea ulterioară a setului de instrumente al UE pentru diplomația cibernetică și pentru a dezvolta instrumente suplimentare pentru a sprijini punerea sa în aplicare. Deși securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru, IA ACT de necesitatea de a consolida schimbul de date operative și de informații și cooperarea între statele membre, precum și cu INTCEN UE, pentru a putea face schimb de date operative la începutul procesului decizional, inclusiv cu privire la chestiunea atribuirii, permițând astfel un răspuns rapid, eficace și întemeiat la activitățile cibernetice răuvoitoare care vizează UE și partenerii săi. REITEREAZĂ importanța consolidării capacității INTCEN UE în domeniul cibernetic, pe baza contribuțiilor voluntare ale statelor membre în materie de date operative și fără a aduce atingere competențelor acestora, precum și a explorării propunerii referitoare la posibila instituire a unui grup de lucru pentru informații cibernetice al statelor membre.

25. RECUNOSCÂND că declarațiile UE și măsurile restrictive luate în cadrul setului de instrumente al UE pentru diplomația cibernetică au transmis un mesaj puternic că activitățile cibernetice răuvoitoare care constituie o amenințare externă la adresa UE, a statelor sale membre și a partenerilor săi sunt inacceptabile și contribuie astfel la prevenirea, descurajarea și răspunsul la activitățile cibernetice răuvoitoare, REITEREAZĂ angajamentul său de a utiliza aceste măsuri pentru a reaminti obligațiile care se aplică spațiului cibernetic în temeiul dreptului internațional, inclusiv al Cartei ONU în integralitatea sa, și de a promova cadrul ONU privind comportamentul responsabil al statelor în spațiul cibernetic, inclusiv obligația privind diligența necesară a tuturor statelor de a nu permite cu bună știință utilizarea teritoriului lor pentru comiterea de fapte ilicite la nivel internațional folosind TIC, în vederea dezvoltării și a promovării în continuare a unei viziuni comune a UE privind aplicarea dreptului internațional în spațiul cibernetic. Constatând că mesajele adecvate și rapide atenuează riscurile de escaladare și pot descuraja atacatorii care vizează interesele europene, INVITĂ Înaltul Reprezentant să elaboreze și să prezinte statelor membre o strategie de comunicare coerentă privind utilizarea setului de instrumente al UE pentru diplomația cibernetică.

26. ÎNCURAJEAZĂ elaborarea unor abordări și răspunsuri treptate, specifice și susținute la activitățile cibernetice răuvoitoare, utilizând gama largă de instrumente oferite de setul de instrumente diplomatice cibernetice al UE, inclusiv regimul UE de sancțiuni cibernetice, și preconizând măsuri suplimentare. SUBLINIAZĂ necesitatea de a spori posibilitatea de a mobiliza, de la caz la caz, toate instrumentele disponibile, interne și externe, pentru a preveni, descuraja și răspunde la atacurile cibernetice, implementându-le printr-o abordare rapidă, eficace, treptată, specifică și susținută, bazată pe un angajament strategic pe termen lung. INVITĂ Înaltul Reprezentant ca, în cooperare cu Comisia, să identifice posibile răspunsuri comune ale UE la atacurile cibernetice, inclusiv opțiuni de sancțiuni, în întregul spectru, astfel încât aceasta să fie pregătită să ia măsuri rapide și eficace atunci când este necesar, și să le prezinte Consiliului până la sfârșitul primului trimestru al anului 2023.

27. Precizând că apărarea cibernetică este în primul rând o responsabilitate națională, ÎNCURAJEAZĂ statele membre să își dezvolte în continuare propriile capabilități de desfășurare a operațiunilor de apărare cibernetică, inclusiv măsuri proactive de detectare și descurajare a atacurilor cibernetice, precum și de protejare și de apărare împotriva acestora și, eventual, în sprijinul altor state membre și al UE. Fiecare stat membru este încurajat să își consolideze, dacă este necesar, propriile capacități de a furniza și de a primi ajutor și asistență. SUBLINIAZĂ că dezvoltarea în continuare a acestor capabilități ar trebui să fie unul dintre obiectivele-cheie ale viitoarei politici de apărare cibernetică a UE. CONSTATĂ că politica de apărare cibernetică a UE ar trebui să acorde mai multă atenție rolului pe care instituțiile și organele relevante ale UE îl pot juca pentru a spori cooperarea dintre actorii relevanți ai UE și ai statelor membre în domeniul apărării cibernetice și pentru a-și dezvolta propriile capacități, în conformitate cu mandatele lor respective. INVITĂ Înaltul Reprezentant, împreună cu Comisia, să completeze dezvoltarea unei poziții cibernetice a UE prin prezentarea unei propuneri ambițioase privind o politică de apărare cibernetică a UE în 2022, care va pregăti terenul pentru dezvoltarea în continuare de către Consiliu a poziției cibernetice a UE.

28. SUBLINIAZĂ necesitatea de a spori interoperabilitatea și schimbul de informații prin cooperarea dintre centrele militare de răspuns la incidente de securitate cibernetică (milCERT). INVITĂ statele membre să creeze, pe baza activității AEA, o rețea MilCERT pentru a dezvolta cooperarea și a facilita schimbul de informații, ceea ce ar contribui, de asemenea, la promovarea coordonării cu alte comunități cibernetice, precum și o rețea a comandanților cibernetici militari în vederea consolidării cooperării strategice între comandamentele cibernetice ale statelor membre ale UE sau alte autorități omoloage. Crearea acestor rețele, împreună cu proiectele PESCO în domeniul cibernetic, ar contribui la consolidarea apărării cibernetice la nivelul UE. Subliniază importanța cooperării dintre rețeaua milCERT propusă și rețeaua civilă (CSIRT) deja existentă pentru a îmbunătăți schimbul de informații și conștientizarea situației.

29. Pe baza Viziunii și strategiei militare privind spațiul cibernetic ca domeniu de operații elaborate de UE și luând act de dezvoltarea permanentă a conceptului militar de apărare cibernetică pentru operațiile și misiunile militare conduse de UE, REITEREAZĂ necesitatea de a integra dimensiunea cibernetică în planificarea și conducerea misiunilor și operațiilor PSAC, inclusiv prin consolidarea capabilităților lor cibernetice, și SUBLINIAZĂ că acest lucru va contribui la o mai bună conștientizare a situației cibernetice la nivelul UE.

30. În concluzie, CONSTATĂ că poziția cibernetică va fi un pas înainte către instituirea unei doctrine a UE privind acțiunea în spațiul cibernetic, bazată pe o consolidare a rezilienței, a capabilităților și a opțiunilor de răspuns, precum și pe o poziție comună privind aplicarea dreptului internațional în spațiul cibernetic. Consiliul VA FACE UN BILANȚ al progreselor înregistrate în ceea ce privește punerea în aplicare a acestor concluzii în 2023, pentru a asigura dezvoltarea în continuare a poziției cibernetice a UE.