Consiliul
Uniunii Europene

Bruxelles, 23 martie 2021
(OR. en)

7290/21

CYBER 80
TELECOM 124
COPEN 144
CODEC 443
COPS 107
COSI 50
CSC 119
CSCI 45
IND 70
RECH 117
ESPACE 21

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	22 martie 2021
Destinatar:	Delegațiile
Subiect:	Concluziile Consiliului privind Strategia de securitate cibernetică a UE pentru deceniul digital - Concluziile Consiliului aprobate de Consiliu la reuniunea sa din 22 martie 2021

În anexă, se pun la dispoziția delegațiilor Concluziile Consiliului privind Strategia de securitate cibernetică a UE pentru deceniul digital, astfel cum au fost aprobate de Consiliu în cadrul reuniunii sale din 22 martie 2021.

ANEXĂ

Concluziile Consiliului privind Strategia de securitate cibernetică a UE pentru deceniul digital

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],

– guvernanța internetului[2],

– Comunicarea comună din 20 noiembrie 2017 către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”[3],

– consolidarea capacităților și a capabilităților în domeniul securității cibernetice în UE[4],

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

– viitorul unei Europe cu un grad ridicat de digitalizare după 2020: „Stimularea competitivității digitale și economice în întreaga Uniune și a coeziunii digitale”[6],

– eforturi complementare de sporire a rezilienței și de contracarare a amenințărilor hibride[7],

– conturarea viitorului digital al Europei[8],

---

1 12109/13.
2 16200/14.
3 14435/17 + COR 1.
4 7737/19.
5 14517/19.
6 9596/19.
7 14972/19.
8 8711/20.

– diplomația digitală[9],

– consolidarea rezilienței și contracararea amenințărilor hibride, inclusiv a dezinformării, în contextul pandemiei de COVID-19[10],

– diplomația cibernetică[11],

– răspunsul coordonat al UE la incidentele și crizele de securitate cibernetică de mare amploare[12],

– un cadru privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare („Setul de instrumente pentru diplomația cibernetică”)[13],

– Orientările privind consolidarea capacităților cibernetice externe ale UE[14],

– o redresare în vederea promovării tranziției către o industrie europeană mai dinamică, rezilientă și competitivă[15],

– securitatea cibernetică a dispozitivelor conectate[16],

– consolidarea sistemului de reziliență cibernetică al Europei și promovarea unui sector al securității cibernetice competitiv și inovator[17] și

– Rezoluția Consiliului privind criptarea – Securitate prin criptare și securitate în pofida criptării[18], precum și

---

9 12804/20.
10 14064/20.
11 6122/15 + COR 1.
12 10086/18.
13 10474/17.
14 10496/18.
15 13004/20.
16 13629/20.
17 14540/16.
18 13084/1/20 REV 1.

– declarația statelor membre din 15 octombrie 2020 intitulată „Construirea următoarei generații de cloud pentru întreprinderi și sectorul public din UE” (*Building the next generation cloud for business and the public sector in the EU*);

AMINTIND Concluziile Consiliului European din 1-2 octombrie 2020 privind COVID-19, piața unică, politica industrială, dimensiunea digitală și relațiile externe[19], precum și cele din 20 iunie 2019 privind dezinformarea și amenințările hibride și privind o nouă agendă strategică 2019-2024[20],

REAMINTIND „Strategia globală pentru politica externă și de securitate a Uniunii Europene – Viziune comună, acțiuni comune: o Europă mai puternică” din 28 iunie 2016,

AMINTIND Comunicarea Comisiei Europene din 19 decembrie 2020 privind conturarea viitorului digital al Europei[21] și Comunicarea Comisiei Europene din 24 iulie 2020 referitoare la Strategia UE privind uniunea securității[22],

AMINTIND Comunicarea comună a Comisiei Europene și a Înaltului Reprezentant din 2 decembrie 2020 privind o nouă agendă UE-SUA pentru o schimbare globală[23],

1. SUBLINIAZĂ faptul că securitatea cibernetică este esențială pentru construirea unei Europe reziliente, verzi și digitale și SALUTĂ Comunicarea comună către Parlamentul European și Consiliu intitulată „Strategia de securitate cibernetică a UE pentru deceniul digital”, care prezintă noul cadru de acțiune a UE în domeniul „rezilienței, suveranității tehnologice și poziției de lider”, precum și în ceea ce privește modalitățile de protejare a cetățenilor, a întreprinderilor și a instituțiilor din Europa împotriva incidentelor și amenințărilor cibernetice, sporind totodată încrederea persoanelor și a organizațiilor în capacitatea UE de a promova o infrastructură și o conectivitate, precum și rețele și sisteme informatice securizate și fiabile, și de a promova și a proteja un spațiu cibernetic deschis, liber, stabil și securizat la nivel mondial, întemeiat pe drepturile omului, libertățile fundamentale, democrație și statul de drept.

---

19 EUCO 13/20.
20 EUCO 9/19.
21 19.2.2020, COM(2020) 67 final.
22 24.7.2020, COM(2020) 605 final.
23 2.12.2020, JOIN(2020) 22 final.

2. RECUNOAȘTE că pandemia de COVID-19 a adus în prim-planul vieții noastre de zi cu zi nevoia tot mai mare de încredere în instrumentele și sistemele tehnologiei informației și comunicațiilor (TIC) și în securitatea acestora. SUBLINIAZĂ că securitatea cibernetică și internetul mondial deschis sunt vitale pentru funcționarea instituțiilor și administrației publice, atât la nivel național, cât și la nivelul UE, precum și pentru societatea noastră și pentru economie în ansamblu.

3. EVIDENȚIAZĂ necesitatea de a spori gradul de conștientizare a aspectelor cibernetice la nivel decizional politic și strategic oferind factorilor de decizie cunoștințe și informații relevante și SUBLINIAZĂ necesitatea de a spori gradul de sensibilizare a publicului larg și de a promova igiena cibernetică.

4. SOLICITĂ promovarea și protejarea valorilor fundamentale ale UE: democrația, statul de drept, drepturile omului și libertățile fundamentale, inclusiv dreptul la libertatea de exprimare și de informare, dreptul la libertatea de întrunire și de asociere și dreptul la viață privată în spațiul cibernetic. SALUTĂ, în acest sens, continuarea eforturilor susținute de protejare a apărătorilor drepturilor omului, a societății civile și a mediului academic care se ocupă de chestiuni precum securitatea cibernetică, confidențialitatea datelor, supravegherea și cenzura online, oferind orientări practice suplimentare, promovând bune practici și intensificând eforturile UE de prevenire a încălcărilor drepturilor omului și a abuzurilor împotriva acestora și totodată a utilizării abuzive a tehnologiilor emergente, în special prin utilizarea de măsuri diplomatice după caz, precum și prin controlul exporturilor de astfel de tehnologii. SUBLINIAZĂ, în acest context, importanța Planului de acțiune al UE privind drepturile omului și democrația 2020-2024 și a Orientărilor UE în domeniul drepturilor omului privind libertatea de exprimare online și offline.

5. EVIDENȚIAZĂ că atingerea autonomiei strategice, menținându-se în același timp o economie deschisă, reprezintă un obiectiv-cheie al Uniunii pentru a-și stabili propria traiectorie economică și interesele economice. Aceasta include consolidarea capacității de a face alegeri autonome în domeniul securității cibernetice, cu scopul de a consolida poziția de lider a UE în domeniul digital și capacitățile sale strategice. REAMINTEȘTE că aceasta include identificarea și reducerea dependențelor strategice și creșterea rezilienței în ecosistemele industriale cele mai sensibile și în domenii specifice. SUBLINIAZĂ că acest lucru poate include diversificarea lanțurilor de producție și de aprovizionare, promovarea și atragerea investițiilor și a producției în Europa, explorarea de soluții alternative și modele circulare și promovarea cooperării industriale la scară largă în toate statele membre.

6. Având în vedere deficitul de competențe digitale și în materie de securitate cibernetică la nivelul forței de muncă, EVIDENȚIAZĂ importanța satisfacerii cererii de forță de muncă instruită în domeniul digital și al securității cibernetice, în special prin dezvoltarea, păstrarea și atragerea celor mai bune talente, de exemplu prin educație și formare, pentru a putea digitaliza societatea noastră într-un mod securizat din punct de vedere cibernetic. ÎNCURAJEAZĂ participarea sporită a femeilor și fetelor la educația în domeniul științelor, tehnologiei, ingineriei și matematicii („STIM") și la perfecționarea profesională în domeniul TIC și la recalificarea în vederea obținerii de competențe digitale drept unul dintre mijloacele de reducere a decalajului digital dintre femei și bărbați.

7. 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 său față de soluționarea litigiilor internaționale privind spațiul cibernetic prin mijloace pașnice și că toate eforturile diplomatice ale UE ar trebui, în mod prioritar, să vizeze promovarea securității și stabilității în spațiul cibernetic printr-o cooperare internațională sporită și reducerea riscului de percepție greșită, de escaladare și de conflict care ar putea decurge din incidente TIC și SPRIJINĂ dezvoltarea în continuare și operaționalizarea măsurilor de consolidare a încrederii (CBM) la nivel regional și internațional. REITEREAZĂ apelul Adunării Generale a Organizației Națiunilor Unite, convenit prin consens, ca statele membre ale ONU să fie ghidate de recomandările rapoartelor Grupului de experți guvernamentali (GEG) al ONU în utilizarea TIC și REAFIRMĂ aplicarea dreptului internațional, în special a Cartei ONU în întregime, în spațiul cibernetic.

8. REAFIRMĂ că, în vederea conturării substanțiale a normelor și standardelor internaționale în domeniul tehnologiilor emergente și al infrastructurii tehnice și logice esențiale pentru disponibilitatea generală și integritatea nucleului public al internetului, astfel încât acestea să fie în conformitate cu valorile universale și ale UE, și printr-o abordare multipartită, este esențială dezvoltarea în continuare a normelor și standardelor în cadrul Uniunii. Acest lucru va garanta că internetul rămâne global, deschis, liber, stabil și securizat și că utilizarea și dezvoltarea tehnologiilor digitale respectă drepturile omului, precum și că utilizarea lor este legală, sigură și etică. IA ACT de viitoarea strategie de standardizare și SE ANGAJEAZĂ să desfășoare activități de informare proactive și coordonate pentru a promova poziția de lider a UE și obiectivele UE la nivel internațional, inclusiv în cadrul diferitelor organisme internaționale de standardizare și prin cooperarea cu parteneri care împărtășesc aceeași viziune, cu societatea civilă, cu mediul academic și cu sectorul privat.

9. SPRIJINĂ FERM modelul multipartit pentru guvernanța internetului și securitatea cibernetică și se angajează să consolideze schimburile regulate și structurate cu părțile interesate, inclusiv cu sectorul privat, cu mediul academic și cu societatea civilă, în cadrul forurilor internaționale, inclusiv în contextul Apelului de la Paris la încredere și securitate în spațiul cibernetic. PROMOVEAZĂ accesul universal, la prețuri accesibile și egal la internet, care să elimine decalajul digital și, în special, capacitarea femeilor și fetelor, precum și a persoanelor aflate în situații vulnerabile sau marginalizate, atât în elaborarea politicilor, cât și în utilizarea internetului.

10. SUBLINIAZĂ necesitatea de a include securitatea cibernetică în investițiile și inițiativele digitale în următorii ani și necesitatea de a contribui treptat la crearea unor condiții de concurență echitabile în domeniul securității cibernetice și IA ACT de planul Comisiei de a crește cheltuielile publice și de a mobiliza investițiile private în domeniul securității cibernetice. EVIDENȚIAZĂ importanța întreprinderilor mici și mijlocii (IMM-uri) în ecosistemul de securitate cibernetică și RECUNOAȘTE instrumentele financiare relevante disponibile pentru a sprijini punerea unui accent puternic pe securitatea cibernetică în contextul transformării digitale pe durata cadrului financiar multianual (CFM) 2021-2027, precum și la nivelul Mecanismului de redresare și reziliență (RRF).

11. AȘTEAPTĂ CU INTERES punerea în aplicare rapidă a Regulamentului privind Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și Rețeaua de centre naționale de coordonare (CCCN), inclusiv înființarea și operaționalizarea rapidă a Centrului european de competențe în materie de securitate cibernetică de la București. Adoptarea promptă a agendei sale va contribui la maximizarea efectelor investițiilor pentru a consolida poziția de lider a Uniunii și autonomia strategică a acesteia în domeniul securității cibernetice, pentru a sprijini competențele și capacitățile tehnologice și pentru a spori competitivitatea globală a Uniunii cu contribuții din partea industriei și a comunităților academice în domeniul securității cibernetice, inclusiv din partea IMM-urilor și a centrelor de cercetare, care vor beneficia de pe urma unei colaborări mai sistematice, mai incluzive și mai strategice, având în vedere coeziunea Uniunii și a tuturor statelor sale membre.

12. SALUTĂ activitatea în curs desfășurată de ENISA, împreună cu statele membre și părțile interesate, pentru a furniza UE sisteme de certificare pentru produsele, serviciile și procesele TIC care ar trebui să contribuie la creșterea nivelului general de securitate cibernetică în cadrul pieței unice digitale. În acest context, AȘTEAPTĂ CU INTERES programul de activitate etapizat la nivelul Uniunii (URWP) în vederea dezvoltării sistemelor UE de certificare a securității cibernetice în cadrul Regulamentului privind securitatea cibernetică (CSA). RECUNOAȘTE, în acest context, rolul central al UE de a elabora standarde care pot contura peisajul securității cibernetice și care contribuie la asigurarea unei concurențe loiale în cadrul UE și pe scena mondială, promovând accesul pe piață, precum și abordând riscurile în materie de securitate, asigurând totodată aplicabilitatea cadrului legislativ al UE.

13. REITEREAZĂ că este important să fie evaluată necesitatea unei legislații orizontale, care să specifice totodată condițiile necesare pentru introducerea pe piață, pentru a aborda pe termen lung toate aspectele relevante ale securității cibernetice a dispozitivelor conectate, cum ar fi disponibilitatea, integritatea și confidențialitatea. SALUTĂ, în acest sens, o discuție pe tema analizării domeniului de aplicare al unei astfel de legislații și a legăturilor sale cu cadrul de certificare a securității cibernetice, astfel cum este definit în CSA, cu scopul de a spori nivelul de securitate în interiorul pieței unice digitale. SUBLINIAZĂ că cerințele în materie de securitate cibernetică ar trebui definite în conformitate cu legislația relevantă a Uniunii, inclusiv CSA, noul cadru legislativ (NLF), Regulamentul privind standardizarea europeană și o posibilă legislație orizontală viitoare, pentru a evita fragmentarea și ambiguitatea în cadrul legislației.

14. RECUNOAȘTE importanța unei abordări cuprinzătoare și orizontale privind securitatea cibernetică în Uniune, respectând totodată pe deplin competențele și nevoile statelor membre, precum și importanța sprijinului continuu pentru asistență tehnică și cooperare în vederea consolidării capacității statelor membre. Ținând seama de evoluția peisajului amenințărilor cibernetice, IA ACT de noua propunere de directivă privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, care se bazează pe Directiva NIS, și își reafirmă sprijinul pentru consolidarea și armonizarea cadrelor naționale în materie de securitate cibernetică și pentru cooperarea susținută dintre statele membre. În plus, SUBLINIAZĂ necesitatea alinierii și a articulării legislației sectoriale în acest domeniu.

15. IA ACT de propunerea Comisiei de a sprijini statele membre în crearea și consolidarea centrelor de operațiuni pentru securitate (SOC) pentru a construi o rețea de SOC în întreaga UE, pentru a monitoriza și a anticipa în continuare semnalele privind posibile atacuri asupra rețelelor. În acest context, AȘTEAPTĂ planurile detaliate ale Comisiei privind rețeaua de SOC, respectând totodată competențele statelor membre. REAMINTEȘTE eforturile depuse de statele membre, sprijinite de UE, pentru a înființa centre de răspuns la incidente de securitate cibernetică (CSIRT) la nivel sectorial, național și regional, precum și centre de schimb de informații și de analiză (ISAC) la nivel național sau european, ca parte a unei rețele eficace de parteneriate în materie de securitate cibernetică în Uniune. AȘTEAPTĂ CU INTERES explorarea potențialului acestei rețele de a consolida SOC, precum și complementaritatea și coordonarea acestora cu rețelele și actorii existenți (în special rețeaua CSIRT), pentru a promova o cultură a unui schimb de informații eficient, securizat și fiabil. SUBLINIAZĂ că acest proces se va baza pe activitatea desfășurată în contextul inițiativelor privind inteligența artificială și calculul de înaltă performanță, precum și pe activitatea desfășurată de centrele europene de inovare digitală.

16. IA ACT de posibila creare a unui sistem de conectivitate securizat, pe baza infrastructurii europene de comunicații cuantice (EuroQCI) și a comunicării guvernamentale prin satelit (Govsatcom) a Uniunii Europene, și RECUNOAȘTE că orice eventuală dezvoltare viitoare ar trebui să se bazeze pe un cadru solid de securitate cibernetică și să ia în considerare întreaga infrastructură de comunicații electronice, cum ar fi sistemele de rețele spațiale, terestre și submarine.

17. AȘTEAPTĂ CU INTERES discuțiile cu Comisia, ENISA, cei doi operatori de servere rădăcină DNS din UE și comunitatea multipartită pentru a evalua rolul celor doi operatori de servere rădăcină DNS din UE în ceea ce privește garantarea faptului că internetul rămâne accesibil și nefragmentat la nivel mondial. SALUTĂ continuarea discuțiilor cu privire la intenția Comisiei de a crea un serviciu european alternativ pentru accesarea internetului mondial (inițiativa „DNS4EU”), bazat pe un model transparent care să fie conform cu cele mai recente standarde și norme în materie de securitate, de protecție a datelor și de protejare a vieții private din faza de proiectare și în mod implicit, pentru a contribui la creșterea rezilienței, menținând și îmbunătățind totodată conectivitatea internațională pentru toate statele membre.

18. RECUNOAȘTE necesitatea unui efort comun din partea Comisiei și a statelor membre pentru a accelera adoptarea unor standarde esențiale privind internetul, inclusiv IPv6, și a unor standarde consacrate în materie de securitate a internetului, întrucât acestea sunt esențiale pentru creșterea nivelului general de securitate, reziliență, deschidere și interoperabilitate a internetului mondial, sporind totodată competitivitatea industriei UE și, în special, a operatorilor de infrastructură de internet.

19. SUBLINIAZĂ importanța unei abordări coordonate, precum și a elaborării și punerii în aplicare a unor măsuri eficace la nivel național pentru a consolida securitatea cibernetică a rețelelor 5G. SPRIJINĂ următoarele etape care trebuie parcurse referitor la securitatea cibernetică a rețelelor 5G, astfel cum sunt prezentate în anexa la Strategia de securitate cibernetică a UE și pe baza rezultatelor raportului privind impactul recomandării Comisiei asupra securității rețelelor 5G, de exemplu în ceea ce privește definirea unei abordări cuprinzătoare și pe termen lung care să vizeze întregul ecosistem și lanț valoric 5G. În vederea consolidării în continuare a abordării coordonate a securității rețelelor 5G, ÎNDEAMNĂ statele membre, instituțiile UE și alte părți interesate relevante să își continue bilanțul periodic, împreună cu schimbul de informații și de bune practici în cadrul fluxului de lucru specific al Grupului de cooperare NIS privind securitatea cibernetică a rețelelor 5G, și să raporteze periodic Consiliului cu privire la progresele înregistrate. EVIDENȚIAZĂ, subliniind totodată responsabilitatea statelor membre pentru protecția securității naționale, angajamentul său ferm de a realiza și de a finaliza rapid punerea în aplicare a măsurilor setului de instrumente al UE pentru securitatea rețelelor 5G și de a continua eforturile depuse pentru a garanta securitatea rețelelor 5G și dezvoltarea generațiilor viitoare de rețele. Cooperarea strânsă dintre statele membre, Comisie și ENISA în ceea ce privește securitatea rețelelor 5G ar putea servi drept exemplu pentru alte aspecte din domeniul securității cibernetice, respectând totodată competențele statelor membre și principiile subsidiarității și proporționalității.

20. RECUNOAȘTE relevanța integrării în continuare a securității cibernetice în mecanismele UE de răspuns la crize și a testării acestora în cadrul unor exerciții relevante și EVIDENȚIAZĂ importanța sporirii cooperării și a schimbului de informații între diferitele comunități cibernetice din cadrul UE și a corelării inițiativelor, structurilor și procedurilor existente [cum ar fi IPCR, rețeaua CSIRT, Grupul de cooperare NIS, Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (CyCLONe), Centrul european de combatere a criminalității informatice, INTCEN UE și alte organisme relevante ale UE] în cazul incidentelor și amenințărilor cibernetice transfrontaliere și de mare amploare. ȚINÂND SEAMA de progresele deja înregistrate în acest domeniu, AȘTEAPTĂ propunerea Comisiei privind procesul, etapele și calendarul pentru definirea Unității cibernetice comune (JCU), cu scopul de a oferi valoare adăugată și un accent clar și de a raționaliza cadrul UE de gestionare a crizelor în materie de securitate cibernetică, inclusiv prin pregătire, conștientizarea comună a situației, consolidarea răspunsului coordonat și a exercițiilor, într-un mod transparent și gradual, evitând în același timp duplicarea și suprapunerea și respectând totodată competențele statelor membre.

21. SUBLINIAZĂ atât importanța promovării cooperării și a schimbului de informații între actorii relevanți din domeniul securității cibernetice și autoritățile competente din domeniul securității și justiției penale, de exemplu autoritățile de aplicare a legii și autoritățile judiciare, cât și necesitatea de a extinde și de a îmbunătăți capacitatea acestor autorități de a investiga și a urmări penal criminalitatea informatică și de a promova negocierile internaționale și normele UE privind accesul transfrontalier la probele electronice. Independent de mediul tehnologic existent la un moment dat, este esențial să se mențină prerogativele autorităților competente în domeniul securității și justiției penale prin asigurarea accesului legal în vederea îndeplinirii atribuțiilor ce le revin, astfel cum este prevăzut și autorizat prin lege. Astfel de legi care prevăd competențe de asigurare a respectării legii trebuie să respecte întotdeauna pe deplin garanțiile procedurale și alte garanții, precum și drepturile fundamentale, în special dreptul la respectarea vieții private și a secretului comunicațiilor și dreptul la protecția datelor cu caracter personal.

22. ÎȘI REAFIRMĂ sprijinul pentru dezvoltarea, punerea în aplicare și utilizarea unei criptări solide ca mijloc necesar de protecție a drepturilor fundamentale și a securității digitale a persoanelor, a guvernelor, a industriei și a societății și, în același timp, RECUNOAȘTE necesitatea de a asigura capacitatea autorităților competente în domeniul securității și justiției penale, de exemplu autoritățile de aplicare a legii și autoritățile judiciare, de a-și exercita competențele legale, atât online, cât și offline, pentru a ne proteja societățile și cetățenii. Autoritățile competente trebuie să poată avea acces la date în mod legal și bine direcționat, cu respectarea deplină a drepturilor fundamentale și a legilor relevante privind protecția datelor, menținând în același timp securitatea cibernetică. SUBLINIAZĂ că orice acțiune întreprinsă trebuie să pună atent în balanță aceste interese cu principiile necesității, proporționalității și subsidiarității.

23. SPRIJINĂ și PROMOVEAZĂ Convenția de la Budapesta privind criminalitatea informatică și lucrările în curs asupra celui de Al doilea protocol adițional la convenția respectivă. În plus, continuă să se angajeze în schimburi multilaterale privind criminalitatea informatică, inclusiv în procesele legate de Consiliul Europei, Biroul Națiunilor Unite pentru Droguri și Criminalitate (UNODC) și Comisia pentru prevenirea criminalității și justiția penală (CCPCJ), pentru a asigura o cooperare internațională sporită în vederea combaterii criminalității informatice, inclusiv schimbul de bune practici și de cunoștințe tehnice și sprijinirea consolidării capacităților, respectând, promovând și protejând în același timp drepturile omului și libertățile fundamentale.

24. Deși securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru, RECUNOAȘTE importanța cooperării strategice în materie de informații cu privire la activitățile și amenințările cibernetice și INVITĂ statele membre, prin intermediul autorităților lor competente, să contribuie în continuare la activitatea INTCEN UE, care funcționează ca centru pentru conștientizarea situației și evaluările amenințărilor în domeniul cibernetic pentru UE, și să analizeze propunerea privind posibila instituire a unui grup de lucru pentru informații cibernetice al statelor membre, pentru a consolida capacitatea specifică a INTCEN în acest domeniu, pe baza contribuțiilor voluntare ale statelor membre în materie de informații și fără a aduce atingere competențelor acestora.

25. EVIDENȚIAZĂ importanța unui cadru de securitate solid și coerent pentru protejarea întregului personal, a tuturor datelor, rețelelor de comunicații și sistemelor informatice ale UE, precum și a proceselor decizionale, pe baza unor norme cuprinzătoare, coerente și omogene. În special, acest lucru ar trebui realizat prin sporirea rezilienței și îmbunătățirea culturii UE în materie de securitate în raport cu amenințările cibernetice și prin consolidarea securității rețelelor UE clasificate și neclasificate, asigurând totodată o guvernanță adecvată și punerea la dispoziție a unor resurse și capacități suficiente, inclusiv în contextul consolidării mandatului CERT-UE. SALUTĂ, în acest context, discuțiile în curs cu privire la stabilirea unor norme comune privind securitatea informațiilor, luând seama în mod corespunzător normele de securitate ale Consiliului pentru protecția informațiilor UE clasificate, precum și definirea unor norme comune obligatorii privind securitatea cibernetică pentru toate instituțiile, organele și agențiile UE.

26. PE BAZA eforturilor UE în materie de diplomație cibernetică, SE ANGAJEAZĂ să sporească eficacitatea și eficiența setului de instrumente pentru diplomația cibernetică și AȘTEAPTĂ CU INTERES aprofundarea discuțiilor cu privire la domeniul său de aplicare și utilizarea sa pe baza lecțiilor învățate din aplicarea până în prezent a acestui instrument. Aceste discuții ar trebui să contribuie la promovarea securității la nivel internațional prin stimularea dialogului și încurajarea unei viziuni comune asupra chestiunilor de securitate cibernetică, prin consolidarea prevenirii, a stabilității, a cooperării și prin promovarea consolidării încrederii și a capacităților și, după caz, prin aplicarea de măsuri restrictive, pentru a preveni, descuraja, înfrâna și răspunde la activitățile cibernetice răuvoitoare care vizează integritatea și securitatea UE și ale statelor sale membre, contribuind astfel la securitatea și stabilitatea internațională și consolidând poziția cibernetică a UE, cu respectarea deplină a competențelor și prerogativelor naționale. În special, ar trebui acordată o atenție deosebită prevenirii și combaterii atacurilor cibernetice cu efecte sistemice care ar putea afecta lanțurile noastre de aprovizionare, infrastructura critică și serviciile esențiale, instituțiile și procesele democratice și ar putea submina securitatea noastră economică, inclusiv prevenirii și combaterii furtului de proprietate intelectuală facilitat prin mijloace informatice. Statele membre și instituțiile UE ar trebui, de asemenea, să reflecteze în continuare asupra articulării dintre cadrul UE de gestionare a crizelor în materie de securitate cibernetică, setul de instrumente pentru diplomația cibernetică și dispozițiile articolului 42 alineatul (7) din TUE și ale articolului 222 din TFUE, în special prin acțiuni bazate pe scenarii, pentru a construi o înțelegere comună a modalităților practice de punere în aplicare a articolului 42 alineatul (7) din TUE.

27. RECUNOAȘTE importanța consolidării cooperării cu organizațiile internaționale și cu țările partenere pentru a promova înțelegerea comună a peisajului amenințărilor cibernetice, pentru a dezvolta dialoguri și mecanisme de cooperare, pentru a identifica, după caz, răspunsuri diplomatice prin cooperare, precum și pentru a îmbunătăți schimbul de informații, inclusiv prin educație, formare și exerciții. În special, EVIDENȚIAZĂ că un parteneriat transatlantic solid în domeniul securității cibernetice contribuie la securitatea, stabilitatea și prosperitatea noastră comună și IA ACT de dispozițiile privind cooperarea în materie de securitate cibernetică din cadrul Acordului comercial și de cooperare UE-Regatul Unit. REAMINTIND 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, reiterează importanța unei cooperări sporite, benefice și care se consolidează reciproc prin educație, formare, exerciții și răspuns coordonat la activitățile cibernetice răuvoitoare, cu respectarea deplină a procedurilor și a autonomiei decizionale ale ambelor organizații, pe baza principiilor transparenței, reciprocității și incluziunii.

28. Pentru a contribui la asigurarea unui spațiu cibernetic global, deschis, liber, stabil și securizat, care are o importanță din ce în ce mai mare pentru prosperitatea, creșterea, securitatea, bunăstarea, conectivitatea și integritatea continuă a societăților noastre, SE ANGAJEAZĂ să se implice permanent în procesele de stabilire a normelor în cadrul organizațiilor internaționale, în special în cadrul proceselor legate de Comisia I a ONU, promovând și contribuind la recunoașterea aplicării dreptului internațional în spațiul cibernetic și la respectarea normelor, regulilor și principiilor unui comportament responsabil al statelor în spațiul cibernetic, inclusiv prin promovarea instituirii rapide a unui program de acțiune (PdA) pentru stimularea comportamentului responsabil al statelor în spațiul cibernetic, ca monitorizare constructivă, incluzivă și bazată pe consens atât a proceselor actuale ale Grupului de experți guvernamentali (GEG) al ONU, cât și a celor ale Grupului de lucru deschis (OEWG) al ONU.

29. REAMINTEȘTE angajamentul său ferm față de multilateralismul eficace și o ordine mondială bazată pe norme, Organizația Națiunilor Unite aflându-se în centrul acesteia, precum și hotărârea sa de a consolida cooperarea și coordonarea cu organizațiile internaționale și regionale, și anume cu sistemul ONU, NATO, CoE, OSCE, OCDE, UA, OAS, ASEAN, ARF, CCG și LSA în ceea ce privește discuțiile pe teme legate de domeniul cibernetic, precum și continuarea și extinderea dialogurilor și consultărilor structurate ale UE în domeniul cibernetic cu țările terțe. SUBLINIAZĂ sprijinul său activ pentru ONU, în special în ceea ce privește Agenda 2030, inclusiv obiectivele de dezvoltare durabilă, și SALUTĂ foaia de parcurs a secretarului general al ONU privind cooperarea digitală și Agenda pentru dezarmare a secretarului general al ONU, care promovează responsabilitatea și aderarea la normele din spațiul cibernetic și contribuie la prevenirea și soluționarea pașnică a conflictelor generate de activitățile răuvoitoare din spațiul cibernetic. SALUTĂ propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate de a institui o rețea informală a diplomației cibernetice a UE, în vederea consolidării implicării și a expertizei atât a UE, cât și a statelor membre cu privire la aspectele cibernetice internaționale, pentru a consolida activitatea coordonată de informare.

30. AȘTEAPTĂ CU INTERES viitoarea propunere de revizuire a cadrului de politici pentru apărarea cibernetică a UE (CDPF) și SE ANGAJEAZĂ să continue eforturile de consolidare a dimensiunilor securității cibernetice și apărării cibernetice, pentru a se asigura că acestea sunt pe deplin integrate în domeniul mai larg al securității și apărării, în special în contextul lucrărilor privind Busola strategică. CONSIDERĂ că viitoarea „Viziune militară și strategie privind spațiul cibernetic ca domeniu de operații” va contribui la aprofundarea acestor discuții. SALUTĂ inițiativa Agenției Europene de Apărare (AEA) de a încuraja cooperarea dintre CERT militare și SPRIJINĂ eforturile depuse pentru a spori sinergiile civilo-militare și coordonarea în domeniul apărării cibernetice și al securității cibernetice, inclusiv în ceea ce privește aspectele legate de spațiu, inclusiv prin intermediul proiectelor PESCO specifice.

31. SALUTĂ propunerea de a elabora o agendă a UE de consolidare a capacităților cibernetice externe, propunerea de a crea un Comitet al UE pentru consolidarea capacităților cibernetice, precum și instituirea și implementarea CyberNet a UE (Rețeaua UE de consolidare a capacităților cibernetice) pentru a spori reziliența cibernetică și capacitățile cibernetice la nivel mondial. În acest context, SALUTĂ cooperarea cu statele membre, precum și cu partenerii din sectorul public și privat, în special Forumul mondial privind competențele cibernetice (GFCE) și alte organisme internaționale relevante, pentru a asigura coordonarea și a evita suprapunerile. În special, ÎNCURAJEAZĂ cooperarea cu partenerii din Balcanii de Vest și din vecinătatea estică și sudică a UE.

32. Pentru a asigura faptul că toate țările pot profita de avantajele sociale, economice și politice ale internetului și ale utilizării tehnologiilor, SE ANGAJEAZĂ să sprijine țările partenere în abordarea provocării tot mai mari reprezentate de activitățile cibernetice răuvoitoare, în special cele care dăunează dezvoltării economiilor, societăților, precum și integrității și securității sistemelor democratice ale acestora, inclusiv în conformitate cu eforturile depuse în cadrul Planului de acțiune pentru democrația europeană.

33. Pentru a asigura elaborarea, punerea în aplicare și monitorizarea propunerilor prezentate în Strategia de securitate cibernetică a UE și ținând seama de caracterul multianual al unora dintre inițiative, ÎNCURAJEAZĂ Comisia și Înaltul Reprezentant pentru afaceri externe și politica de securitate să instituie un plan detaliat de punere în aplicare care să stabilească prioritățile și calendarul acțiunilor planificate. VA MONITORIZA progresele înregistrate în punerea în aplicare a prezentelor concluzii prin intermediul unui plan de acțiune care va fi revizuit și actualizat periodic de către Consiliu, în strânsă cooperare cu Comisia Europeană și cu Înaltul Reprezentant.