Consiliul
Uniunii Europene

**Bruxelles, 20 noiembrie 2017**
**(OR. en)**

**14435/17**

**CYBER 183**
**TELECOM 303**
**ENFOPOL 534**
**JAI 1055**
**MI 845**
**COSI 283**
**JAIEX 101**
**RELEX 989**
**IND 317**
**CSDP/PSDC 643**
**COPS 360**
**POLMIL 145**

**REZULTATUL LUCRĂRILOR**

| | |
|---|---|
| Sursă: | Secretariatul General al Consiliului |
| Data: | 20 noiembrie 2017 |
| Destinatar: | Delegațiile |
| Nr. doc. ant.: | 13943/17 + COR 1 |
| Nr. doc. Csie: | 12210/17, 12211/17 |
| Subiect: | Concluziile Consiliului privind comunicarea comună către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”<br>- Concluziile Consiliului (20 noiembrie 2017) |

În anexă, se pun la dispoziția delegațiilor concluziile Consiliului privind comunicarea comună către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”, adoptate de Consiliul Afaceri Generale la 20 noiembrie 2017.

**ANEXĂ**

**Proiect de concluzii ale Consiliului privind comunicarea comună către PE și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”**

Consiliul Uniunii Europene,

1. RECUNOSCÂND importanța securității cibernetice pentru prosperitatea, creșterea economică și securitatea UE și pentru integritatea societăților noastre libere și democratice și a proceselor care stau la baza acestora în era digitală, prin protejarea atât a statului de drept, cât și a drepturilor omului și a libertăților fundamentale ale fiecăruia;

2. SUBLINIIND necesitatea de a aborda securitatea cibernetică într-un mod coerent la nivel național, la nivelul UE și la nivel mondial, deoarece amenințările cibernetice pot avea consecințe asupra democrației, prosperității, stabilității și securității;

3. IA ACT de faptul că un nivel ridicat de reziliență cibernetică în întreaga UE este, de asemenea, important pentru obținerea încrederii în piața unică digitală și dezvoltarea în continuare a unei Europe digitale;

4. REITERÂND faptul că UE va promova necontenit un spațiu cibernetic deschis, global, liber, pașnic și sigur, în care drepturile omului și libertățile fundamentale, în special dreptul la libertatea de exprimare, accesul la informații, protecția datelor, viața privată și securitatea, precum și valorile și principiile fundamentale ale UE, să fie, atât în cadrul UE, cât și la nivel global, puse în aplicare și respectate pe deplin și SUBLINIIND importanța crucială a asigurării unui echilibru adecvat între drepturile omului și libertățile fundamentale și a respectării cerințelor politicii de securitate internă a UE[1],

5. RECUNOSCÂND că dreptul internațional, inclusiv Carta ONU în deplinătatea sa, și dreptul internațional umanitar și al drepturilor omului se aplică spațiului cibernetic și, prin urmare, SUBLINIIND necesitatea continuării eforturilor pentru asigurarea faptului că dreptul internațional este respectat în spațiul cibernetic;

[1] Doc. 12650/17.

6. REAMINTIND concluziile sale referitoare la strategia de securitate cibernetică a UE[2], la guvernanța internetului[3], la consolidarea sistemului de reziliență cibernetică al UE[4], la diplomația cibernetică[5] și la un cadru privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare[6], la îmbunătățirea justiției penale în spațiul cibernetic[7]; la securitatea și apărarea în contextul Strategiei globale a UE[8], la Cadrul comun privind contracararea amenințărilor hibride[9] și la evaluarea la jumătatea perioadei a Strategiei reînnoite de securitate internă a Uniunii Europene pentru perioada 2015-2020[10];

7. RECUNOSCÂND că prin cadrul oferit de Convenția Consiliului Europei privind criminalitatea informatică (Convenția de la Budapesta) se asigură o bază solidă în rândul unui grup eterogen de țări pentru a utiliza un standard juridic eficace pentru diferitele legislații naționale și pentru cooperarea internațională care abordează criminalitatea informatică;

8. RECUNOSCÂND necesitatea unui accent reînnoit pe punerea în aplicare a cadrului de politici pentru apărarea cibernetică a UE din 2014 și a actualizării acestuia cu scopul de a crește integrarea securității și a apărării cibernetice în cadrul politicii de securitate și apărare comune (PSAC) și în agenda mai amplă în materie de securitate și apărare;

9. RECUNOSCÂND că o industrie europeană competitivă la nivel mondial reprezintă un element important în vederea atingerii unui nivel ridicat de securitate cibernetică la nivel național și la nivelul UE;

10. REAMINTIND că, în conformitate cu articolul 4 alineatul (2) din TUE, securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru.

---

2 Doc. 12109/13 și doc. 6225/13 (Comunicare comună către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat [COM JOIN (2013) 1 final].

3 Doc. 16200/14 și doc. 6460/14 - Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: Guvernanța și politica în domeniul internetului: Rolul Europei în modelarea viitorului guvernanței internetului [COM (2014) 72 final].

4 Doc. 14540/16 și doc. 11013/16 - Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: Consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator [COM 2016(410) final].

5 Doc. 6122/15.

6 Doc. 9916/17.

7 Doc. 10007/16.

8 Doc. 9178/17.

9 Doc. 7688/16 (Comunicare comună către Parlamentul European și Consiliu intitulată „Cadrul comun privind contracararea amenințărilor hibride: un răspuns al Uniunii Europene”).

10 Doc. 12650/17.

**PRIN PREZENTA**

11. SALUTĂ Comunicarea comună către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE” pentru faptul că propune un obiectiv ambițios de îmbunătățire a securității cibernetice în cadrul UE. Aceasta contribuie, de asemenea, la autonomia strategică a UE, astfel cum se menționează în concluziile sale privind Strategia globală pentru politica externă și de securitate a Uniunii Europene[11], prin obiectivul urmărit de a construi o Europă digitală care va fi mai sigură, va favoriza încrederea, va fi conștientă de punctele sale forte, competitivă şi deschisă către lume şi va respecta valorile comune ale UE referitoare la un internet la nivel mondial deschis, liber, pașnic și sigur și, prin urmare, contribuie la atingerea unui nivel mai ridicat de reziliență cu scopul de a preveni, a descuraja, a depista și a răspunde la amenințările cibernetice, precum și de a face posibil un răspuns comun la amenințări cibernetice în întreaga UE, și

12. INVITĂ statele membre, instituțiile, agențiile și organismele UE să colaboreze, cu respectarea domeniilor de competență ale fiecăruia și a principiului subsidiarității și al proporționalității, ca răspuns la obiectivele strategice stabilite în prezentele concluzii, și

13. SUBLINIAZĂ necesitatea ca UE, statele sale membre și sectorul privat să asigure o finanțare suficientă, respectând resursele disponibile, pentru a sprijini consolidarea rezilienței cibernetice și eforturile de cercetare și dezvoltare în domeniul securității cibernetice în întreaga UE, precum și pentru a consolida cooperarea pentru a preveni, a descuraja, a detecta și a răspunde la amenințările cibernetice, precum și pentru a face posibil un răspuns comun la incidente cibernetice la scară largă și la activități cibernetice răuvoitoare în întreaga UE;

[11] Doc. 13202/16.

**Capitolul I**

**ASIGURAREA UNEI REZILIENȚE CIBERNETICE A UE EFICACE ȘI A ÎNCREDERII ÎN PIAȚA UNICĂ DIGITALĂ**

14. SUBLINIAZĂ că fiecare stat membru poartă responsabilitatea primară pentru îmbunătățirea propriei sale securități cibernetice și asigurarea răspunsului său la incidente și crize cibernetice, în timp ce UE poate oferi o valoare adăugată considerabilă prin sprijinirea cooperării între statele membre. În acest context, SUBLINIAZĂ necesitatea ca toate statele membre să pună resursele necesare la dispoziția autorităților naționale responsabile în materie de securitate cibernetică pentru a asigura prevenirea și detectarea incidentelor și crizelor cibernetice în întreaga UE, precum și răspunsul la acestea;

15. SUBLINIAZĂ necesitatea recurgerii, acolo unde este posibil, la mecanismele, structurile și organizațiile existente la nivelul UE;

16. SALUTĂ:

- progresele înregistrate în transpunerea Directivei privind securitatea cibernetică de către statele membre și SUBLINIAZĂ necesitatea realizării unei puneri în aplicare integrale și efective până în mai 2018, astfel cum este prevăzut în directiva respectivă[12];
- lucrările desfășurate în cadrul grupului de cooperare privind securitatea rețelelor și a informațiilor cu scopul de a spori cooperarea strategică și schimbul de informații dintre statele membre;
- activitatea desfășurată în cadrul rețelei CSIRT, în special în ceea ce privește consolidarea cooperării operaționale a statelor membre, consolidarea încrederii în schimbul de informații în cadrul gestionării incidentelor de securitate cibernetică de mare amploare și, pe baza concluziilor naționale din partea statelor membre, furnizarea de elemente pentru o conștientizare comună a situației la nivel european;
- lucrările desfășurate în cadrul parteneriatului public-privat contractual (PPPc) privind securitatea cibernetică.

[12] Fără a aduce atingere competenței statelor membre pentru transpunerea Directivei privind securitatea cibernetică, în special în ceea ce privește operatorii de servicii esențiale.

17. SALUTĂ confirmarea în comunicarea comună a faptului că un sistem de criptare puternic şi de încredere este extrem de important pentru asigurarea în mod adecvat a respectării drepturilor omului și a libertăților fundamentale în UE și pentru încrederea publicului în piața unică digitală, ținând seama în același timp de nevoia autorităților de aplicare a legii de a accesa date necesare pentru propriile anchete, precum și confirmarea faptului că atât identificarea, cât și comunicarea digitală sigură joacă un rol esențial în garantarea unei securități cibernetice efective în UE;

18. SALUTĂ planul din comunicarea comună privind creşterea nivelului de ambiţie în desfășurarea în mod regulat a exercițiilor de securitate cibernetică paneuropene, bazându-se pe experiențele acumulate în urma exercițiilor Cyber Europe şi combinând reacțiile de la diferite niveluri, deoarece acesta va constitui un element important pentru îmbunătățirea nivelului de pregătire a statelor membre și a instituțiilor UE pentru a face față incidentelor cibernetice de mare amploare;

19. INVITĂ UE și statele sale membre să desfășoare periodic exerciții strategice de securitate cibernetică în diferite formațiuni ale Consiliului, bazându-se pe experiența dobândită în cursul EU CYBRID 2017, și

20. Fără a aduce atingere rezultatului procesului legislativ:

- SALUTĂ propunerea referitoare la un mandat puternic și permanent pentru ENISA cu obiectivul principal de a sprijini și a dezvolta o cooperare mai strânsă între statele membre, pentru a le crește capacitățile și pentru a spori încrederea în Europa digitală;

- REAFIRMĂ faptul că viitoarea ENISA ar trebui să se bazeze pe experiența și cunoștințele de specialitate din statele membre și UE și să sprijine dezvoltarea și punerea în aplicare cu consecvență a politicilor și reglementărilor existente și viitoare ale UE în materie de securitate cibernetică, asigurându-se, în același timp, ca toate competențele ENISA să fie dezvoltate pentru a le completa pe cele ale statelor membre;

- REAFIRMĂ obiectivul sporirii încrederii în Europa digitală prin creșterea încrederii în soluțiile și inovațiile digitale, inclusiv internetul obiectelor, comerțul electronic și e-guvernanța, în special din perspectiva unui cadru european de talie mondială de certificare a securității cibernetice[13]. Aceasta este o cerință-cheie pentru consolidarea încrederii și a securității în produsele și serviciile digitale și pentru protejarea infrastructurilor critice și a datelor administrațiilor publice, ale cetățenilor și ale întreprinderilor și o cerință esențială pentru adoptarea unei abordări de tipul „securitate de la stadiul conceperii” pentru produsele, serviciile și procesele din cadrul pieței unice digitale;

- SUBLINIAZĂ că activitatea legislativă menită să consolideze certificarea securității cibernetice la nivelul UE va trebui să satisfacă nevoile pieței și ale utilizatorilor și să se bazeze pe experiențele legate de capacitățile și procesele de certificare existente în UE (de exemplu cadrul SOG-IS) și ar trebui să ofere un cadru capabil să se adapteze rapid la viitoarele evoluții digitale de ultimă generație;

- SUBLINIAZĂ că, în cadrul consolidării certificării securității cibernetice în UE, ar trebui să fie acoperit întregul spectru de cerințe în materie de securitate, până la cele mai înalte, acolo unde trebuie demonstrată rezistența împotriva capacităţilor atacatorilor. Printre factorii de succes esențiali s-ar număra asigurarea unui proces fiabil, transparent și independent pentru certificarea securității în vederea promovării disponibilității dispozitivelor, a programelor informatice și a serviciilor de încredere şi sigure în cadrul pieței unice și în afara ei; recunoaşterea expertizei industriei, a administraţiilor publice și, respectiv, a specialiștilor în materie de evaluare de la nivel european prin standarde europene și mondiale[14]; respectarea rolului statelor membre în procesul de certificare, în special în ceea ce privește evaluarea la niveluri de securitate mai înalte și mai ales în legătură cu nevoile esențiale în materie de securitate și cu evaluarea competențelor. Un astfel de cadru de certificare ar trebui, de asemenea, să asigure faptul că orice sistem de certificare la nivelul UE este proporțional cu nivelul de asigurare necesar pentru utilizarea produselor, a serviciilor și/sau a sistemelor TIC implicate și permite comerțul transfrontalier pentru întreprinderile de toate mărimile astfel încât acestea să dezvolte și să comercializeze produse noi, atât în cadrul UE, cât și pe pieţele din afara UE.

---

**13** Prin intermediul unor standarde globale elaborate în spiritul Codului de bune practici din Acordul BTC al OMC.

**14** Prin intermediul unor standarde europene şi globale elaborate în spiritul Codului de bune practici din Acordul BTC al OMC.

21. SALUTĂ intenția de a se institui o rețea a centrelor de competență în materie de securitate cibernetică pentru a stimula dezvoltarea și implementarea de tehnologii în materie de securitate cibernetică, precum și pentru a oferi un impuls suplimentar inovării pentru industria UE pe scena mondială în ceea ce privește dezvoltarea următoarei generații de tehnologii inovatoare, precum inteligența artificială, informatica cuantică, blockchain și identitățile digitale sigure;

22. SUBLINIAZĂ că este necesar ca rețeaua centrelor de competență în materie de securitate cibernetică să fie deschisă participării tuturor statelor membre și centrelor acestora de excelență și de competență existente, precum și să acorde o atenție deosebită complementarității și, ținând cont de acest aspect, IA ACT de planul de creare a centrului european de cercetare în materie de securitate cibernetică, care ar trebui să aibă rolul-cheie de a se concentra asupra asigurării complementarității și asupra evitării suprapunerilor în cadrul rețelei centrelor de competență în materie de securitate cibernetică și cu alte agenții ale UE;

23. SUBLINIAZĂ că rețeaua centrelor de competență în materie de securitate cibernetică ar trebui să abordeze o gamă de aspecte, de la cercetare la industrie, și, prin urmare, ar trebui să contribuie, printre altele, la îndeplinirea obiectivului autonomiei strategice europene;

24. Cu privire la rețeaua centrelor de competență în materie de securitate cibernetică propusă, REAFIRMĂ că este necesar ca UE, prin intermediul statelor sale membre, să dezvolte o capacitate europeană pentru a evalua soliditatea criptografiei utilizate în produsele și serviciile disponibile pentru cetățeni, întreprinderi și administrațiile publice pe piața unică digitală, recunoscând, în același timp, că politicile în materie de criptografie reprezintă un aspect esențial al securității naționale și intră astfel în sfera de competență a statelor membre;

25. INVITĂ toate părțile interesate relevante să sporească investițiile în aplicaţiile de securitate cibernetică ale noilor tehnologii, pentru a contribui la asigurarea securității cibernetice în toate sectoarele economiei europene;

26. SUBLINIAZĂ importanța furnizării unor servicii de securitate cibernetică credibile, fiabile și coordonate în beneficiul instituțiilor UE și FACE APEL la COMISIE și la alte instituții ale UE să dezvolte în continuare CERT-UE ținând seama de aceste obiective și să asigure, de asemenea, un nivel adecvat de resurse în acest scop;

27. SALUTĂ apelul lansat în vederea recunoașterii rolului important al cercetătorilor terți în domeniul securității în descoperirea vulnerabilităților prezente în produsele și serviciile existente și INVITĂ statele membre să facă schimb de bune practici în ceea ce privește divulgarea coordonată a vulnerabilității;

28. INSISTĂ asupra responsabilității fiecăruia în domeniul securității cibernetice și INVITĂ UE și statele sale membre să promoveze competențele digitale și alfabetizarea mediatică care să îi ajute pe utilizatori să își protejeze informațiile digitale în mediul online și să îi sensibilizeze într-o mai mare măsură în ceea ce privește riscurile la care se expun atunci când publică pe internet date cu caracter personal;

29. SALUTĂ accentul pus în comunicarea comună pe educație, pe igiena cibernetică și pe gradul de conștientizare în statele membre și în UE;

30. INVITĂ COMISIA să prezinte în scurt timp o evaluare a impactului cu privire la punerea în aplicare a inițiativei de instituire a unei rețele de centre de competență în materie de securitate cibernetică și a unui centru european de competență și de cercetare în materie de securitate cibernetică, precum și să propună, până la jumătatea lui 2018, instrumentele legislative relevante pentru punerea în aplicare a inițiativei;

31. INVITĂ statele membre:

- să acorde prioritate sensibilizării cu privire la securitatea cibernetică în campaniile de informare și să încurajeze includerea securității cibernetice în cadrul programelor de formare academică, educațională și profesională. Ar trebui pus un accent deosebit pe educația tinerilor și pe promovarea competențelor digitale, cu scopul de a forma specialiști pregătiți pentru provocările viitoare în materie de securitate, economie și servicii;

- să promoveze eforturile depuse în vederea lansării unor programe specializate la nivel înalt în materie de securitate cibernetică pentru a compensa lacunele existente în ceea ce privește specialiștii în domeniul securității cibernetice din UE;

- să creeze o rețea de cooperare eficace alcătuită din puncte de contact în domeniul educației sub egida ENISA. Rețeaua de puncte de contact ar trebui să aibă drept obiectiv consolidarea coordonării și a schimbului de bune practici între statele membre în ceea ce privește educația și sensibilizarea cu privire la securitatea cibernetică, precum și formarea, exercițiile și consolidarea capacităților;

- să ia în considerare aplicarea normelor prevăzute în Directiva privind securitatea cibernetică, inclusiv în administrațiile publice care participă la activități economice și societale vitale, în cazul în care acestea nu intră deja sub incidența legislației naționale și dacă se consideră necesar, și să furnizeze stagii de formare în domeniul securității cibernetice inclusiv în administrațiile publice, dat fiind rolul pe care acestea îl joacă în cadrul societății și al economiei noastre.

**Capitolul II**

**CONSOLIDAREA CAPACITĂȚII UE DE A PREVENI, A DESCURAJA, A DEPISTA ȘI A RĂSPUNDE LA ACTIVITĂȚILE CIBERNETICE RĂUVOITOARE**

32. SUBLINIAZĂ faptul că un incident sau o criză cibernetică deosebit de gravă ar putea constitui un motiv suficient pentru ca un stat membru să invoce clauza de solidaritate a UE[15] și/sau clauza de asistență reciprocă[16];

33. SALUTĂ adoptarea „Cadrului privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare”, care contribuie la prevenirea conflictelor, la cooperare și stabilitate în spațiul cibernetic prin stabilirea de măsuri care țin de PESC, inclusiv măsuri restrictive, care pot fi utilizate pentru a preveni și a răspunde la activități cibernetice răuvoitoare, și SOLICITĂ SEAE și statelor membre să acționeze periodic în limitele acestui cadru;

---

[15] Articolul 222 TFUE.
[16] Articolul 42.7 din TFUE

34. SUBLINIAZĂ necesitatea unui răspuns eficace la nivelul UE la incidentele și crizele cibernetice de mare amploare, respectând în același timp competențele statelor membre, precum și necesitatea integrării securității cibernetice în mecanismele existente de gestionare a crizelor la nivelul UE[17]. În acest scop, SOLICITĂ exersarea periodică a răspunsului la nivelul UE la incidentele cibernetice de mare amploare - de la răspunsul diplomatic-strategic la cel de ordin tehnic - pornind de la cadrele și procedurile relevante, precum și în urma ajustării acestora, după caz[18];

35. SUBLINIAZĂ importanța unor mecanisme de răspuns și de schimb de informații bine integrate între diferitele comunități care sunt esențiale pentru asigurarea securității cibernetice în Europa, inclusiv între organismele relevante ale UE și autoritățile statelor membre. Va trebui ca aceste mecanisme să fie testate și verificate ca parte din exercițiile în materie de securitate cibernetică desfășurate la nivelul UE, precum și oficializate prin acorduri corespunzătoare, dacă va fi necesar;

36. IA ACT de posibilitatea de a examina, în cazul în care Comisia ar prezenta o propunere pentru instituirea unui fond de răspuns la situații de urgență legate de securitatea cibernetică în completarea eforturilor întreprinse deja de statele membre, precum și cu respectarea resurselor disponibile (în special în limitele cadrului financiar multianual al UE), ajutorul acordat statelor membre pentru ca acestea să răspundă la incidentele cibernetice de mare amploare și să atenueze impactul acestora, cu condiția ca statul membru să fi instituit un sistem prudent de securitate cibernetică înainte de incident, care să includă punerea în aplicare pe deplin a Directivei privind securitatea cibernetică și existența la nivel național a unor cadre consolidate de gestionare a riscurilor și de supraveghere ;

37. RECUNOAȘTE legătura tot mai strânsă dintre securitatea cibernetică și apărare și SOLICITĂ intensificarea cooperării în domeniul apărării cibernetice, inclusiv prin încurajarea cooperării dintre comunitățile civile și militare de răspuns în caz de incidente, precum și continuarea consolidării securității cibernetice a misiunilor și operațiilor PSAC;

---

**17** Doc. C/2017/6100 final

**18** Doc. 9916/17 și C/2017/6100 final.

38. SUBLINIAZĂ necesitatea de a valorifica pe deplin, după caz, inițiativele propuse în domeniul apărării de a accelera dezvoltarea unor capabilități cibernetice adecvate în Europa și RECUNOAȘTE oportunitățile oferite de eventuala dezvoltare a unor proiecte de apărare cibernetică prin intermediul PESCO, dacă statele membre care participă la PESCO consideră că este necesar, și RECUNOAȘTE rolul jucat de baza industrială și tehnologică de apărare europeană (EDTIB) și de baza industrială în domeniul securității cibernetice civile în general în punerea la dispoziția statelor membre a unor mijloace de a-și proteja interesele în domeniul securității și apărării cibernetice;

39. IA ACT de propunerea Comisiei de a institui o platformă educațională și de formare în domeniul apărării cibernetice până la sfârșitul anului 2018 și SUBLINIAZĂ că platforma ar trebui să sporească oportunitățile în materie de educație și formare din statele membre și ar trebui să asigure complementaritatea cu alte eforturi și inițiative ale UE, în special cu CESA și AEA;

40. FACE APEL la UE și la statele sale membre să reacționeze la amenințarea reprezentată de furtul de proprietate intelectuală prin intermediul TIC, inclusiv furtul de secrete comerciale sau de alte informații comerciale confidențiale, cu intenția de a oferi avantaje competitive unor întreprinderi sau unor sectoare comerciale;

41. RECUNOAȘTE necesitatea de a aborda infracțiunile din spațiul cibernetic, inclusiv cele comise în Darkweb, exploatarea sexuală a copiilor în spațiul online, precum și frauda și falsificarea mijloacelor de plată fără numerar, urmărind în special crearea unei imagini de ansamblu îmbunătățite în materie de informații, desfășurarea de investigații comune și sprijinul operațional în comun;

42. SALUTĂ eforturile depuse de UE și de statele sale membre în abordarea provocărilor reprezentate de sistemele care le permit infractorilor și teroriștilor să comunice în moduri pe care autoritățile competente nu le pot accesa; SUBLINIAZĂ că aceste eforturi trebuie să țină seama de faptul că criptarea solidă și sigură este deosebit de importantă pentru securitatea cibernetică și pentru încrederea în piața unică digitală, precum și pentru asigurarea respectării drepturilor omului și a libertăților fundamentale;

43. SUBLINIAZĂ importanța punerii la dispoziția autorităților de aplicare a legii a unor instrumente care să permită depistarea, anchetarea și urmărirea în instanță a criminalității cibernetice, astfel încât infracțiunile comise în spațiul cibernetic să nu treacă neobservate sau să rămână nepedepsite și SALUTĂ contribuția adusă în combaterea criminalității de Rețeaua judiciară europeană de combatere a criminalității informatice prin intermediul cooperării la nivelul autorităților judiciare;

44. SUBLINIAZĂ importanța asigurării unei poziții coordonate la nivel UE pentru conturarea în mod eficace în cadrul comunității multipartite a deciziileorluate la nivel european și global în materie de guvernanță a internetului, cum ar fi asigurarea unor baze de date de tip WHOIS de adrese IP și de nume de domenii, rapid accesibile și precise, astfel încât capabilitățile în materie de aplicare a legii și interesele publice să fie protejate;

45. SUBLINIAZĂ importanța asimilării protocolului de internet IPv6, care este esențial pentru dezvoltarea la scară largă a internetului obiectelor, precum și pentru îmbunătățirea identificării autorilor infracțiunilor comise în spațiul cibernetic;

46. ÎNCURAJEAZĂ activitățile în curs desfășurare în ceea ce privește accesul transfrontalier la probe electronice, în legătură cu păstrarea datelor, precum și în ceea ce privește provocările întâmpinate de procedurile penale reprezentate de sisteme care le permit infractorilor și teroriștilor să comunice în moduri pe care autoritățile competente nu le pot accesa, ținând cont de necesitatea respectării drepturilor omului și a libertăților fundamentale și de protecția datelor;

47. INVITĂ Comisia:

- să prezinte, până în decembrie 2017, un raport privind progresele înregistrate în punerea în aplicare a măsurilor practice de îmbunătățire a accesului transfrontalier la probe electronice;

- să prezinte, la începutul anului 2018, o propunere legislativă care să vizeze îmbunătățirea accesului transfrontalier la probe electronice;

48. INVITĂ Europol, ENISA și Eurojust:

- să continue procesul de consolidare a cooperării în ceea ce privește combaterea criminalității cibernetice, atât între ele, cât și cu alte părți interesate relevante, inclusiv cu comunitatea CSIRT, cu Interpolul, cu sectorul privat și cu mediul academic, prin asigurarea sinergiilor și a complementarităților, în conformitate cu mandatele și competențele fiecărei părți implicate.

- să contribuie, alături de statele membre, la elaborarea unei abordări coordonate a autorităților de aplicare a legii de la nivelul UE în ceea ce privește răspunsul la incidente și crize cibernetice de mare amploare, care să completeze procedurile prevăzute în cadrele relevante[19];

49. INVITĂ UE și statele sale membre să depună în continuare eforturi pentru:

- a elimina obstacolele cu care se confruntă cercetarea penală și justiția penală eficace în spațiul cibernetic, precum și pentru a consolida cooperarea și coordonarea internațională în combaterea criminalității în spațiul cibernetic;

- a aborda provocările reprezentate de tehnologiile de anonimizare, ținând seama totodată de faptul că criptarea solidă și sigură este esențială pentru securitatea cibernetică și pentru încrederea în piața unică digitală;

- a elabora decizii privind guvernanța internetului care să aibă un impact asupra capacității autorităților de aplicare a legii de a combate criminalitatea în spațiul cibernetic;

[19] Doc. 9916/17 și C/2017/6100 final.

**Capitolul III**

**CONSOLIDAREA COOPERĂRII INTERNAȚIONALE PENTRU UN SPAȚIU CIBERNETIC DESCHIS, LIBER, PAȘNIC ȘI SIGUR LA NIVEL GLOBAL**

50. RECUNOAȘTE că asigurarea securității cibernetice este o provocare globală care necesită o cooperare eficace la nivel mondial între toți actorii și RECUNOAȘTE că trebuie acordată o atenție deosebită susținerii valorilor democratice și principiilor unui spațiu cibernetic deschis, liber, pașnic și sigur la nivel global, și, în acest sens,

51. FACE APEL la UE și la statele sale membre să susțină instituirea unui cadru strategic pentru prevenirea conflictelor, cooperare și stabilitate în spațiul cibernetic, care să se bazeze pe aplicarea dreptului internațional existent, în special pe Carta ONU în deplinătatea sa, elaborarea și punerea în aplicare a unor norme universal valabile în materie de comportament statal responsabil, precum și elaborarea unor măsuri regionale de consolidare a încrederii între state;

52. RECUNOAȘTE rolul Organizației Națiunilor Unite în dezvoltarea în continuare a unor norme în ceea ce privește un comportament statal responsabil în spațiul cibernetic și reamintește că rezultatele dezbaterilor desfășurate de-a lungul anilor la nivelul grupului de experți guvernamentali al ONU s-au concretizat într-un set de norme și recomandări consensuale[20], pe care Adunarea generală le-a aprobat în repetate rânduri și pe care statele ar trebui să le considere drept reper pentru un comportament statal responsabil în spațiul cibernetic;

53. RECUNOAȘTE că aceste norme privind un comportament statal responsabil cuprind prevederi conform cărora statele nu ar trebui să permită ca, în cunoștință de cauză, teritoriul lor să fie utilizat pentru fapte ilicite la nivel internațional, ar trebui să dea curs cererilor legitime de asistență formulate de un alt stat a cărui infrastructură critică face obiectul unor fapte răuvoitoare bazate pe TIC provenite de pe teritoriul lor și că statele ar trebui să ia măsuri adecvate pentru a-și proteja infrastructura critică de amenințările din domeniul TIC;

54. RECUNOAȘTE amenințările și riscurile cibernetice comune cu care se confruntă UE, NATO și statele lor membre respective și REITEREAZĂ importanța continuării cooperării dintre UE și NATO în ceea ce privește securitatea cibernetică și apărarea, respectând pe deplin principiile incluziunii, reciprocității și autonomiei decizionale a UE și în conformitate cu Concluziile Consiliului din 6 decembrie 2016 privind punerea în aplicare a declarației comune a președintelui Consiliului European, președintelui Comisiei Europene și secretarului general al Organizației Tratatului Atlanticului de Nord[20];

55. INVITĂ UE și statele sale membre să sprijine și să încurajeze elaborarea unor măsuri de consolidare a încrederii la nivel regional, care reprezintă un element esențial pentru sporirea cooperării și a transparenței și pentru reducerea riscului de conflict. Punerea în aplicare a unor măsuri de consolidare a încrederii în domeniul securității cibernetice în contextul OSCE și în alte contexte regionale va spori gradul de previzibilitate a comportamentului statal și va contribui și mai mult la stabilizarea spațiului cibernetic;

56. REAFIRMĂ faptul că UE va continua să susțină valorile sale fundamentale prin protejarea drepturilor omului și a libertăților fundamentale în temeiul Orientărilor UE privind drepturile omului în ceea ce privește libertatea în mediul online. UE subliniază, de asemenea, importanța implicării în guvernanța internetului a tuturor părților interesate, inclusiv a mediului academic, a societății civile și a sectorului privat;

57. FACE APEL la UE și la statele sale membre să promoveze consolidarea capacităților cibernetice în țările terțe, acordând o prioritate deosebită țărilor care se învecinează cu UE și țărilor în curs de dezvoltare care se confruntă cu o creștere rapidă a conectivității, în vederea abordării criminalității cibernetice și a consolidării rezilienței cibernetice, cu respectarea valorilor fundamentale ale UE. În vederea promovării eforturilor UE în acest domeniu, ar trebui să fie instituită o rețea UE de consolidare a capacităților cibernetice și să fie elaborat un set de orientări ale UE privind consolidarea capacităților cibernetice, care ar trebui să vină în completarea mecanismelor și structurilor existente;

[20] Doc. 15283/16.

58. SUBLINIAZĂ progresele înregistrate în cooperarea UE-NATO în domeniul apărării cibernetice și al securității cibernetice, în ceea ce privește formarea, educația și elaborarea de concepte, evitând, în același timp, dublarea inutilă a eforturilor în cazul în care necesitățile se suprapun, precum și în ceea ce privește promovarea interoperabilității prin standarde și cerințe în materie de apărare cibernetică, și FACE APEL la continuarea cooperării în cadrul unor exerciții în domeniul apărării cibernetice (la nivel de personal) și la efectuarea unui schimb de bune practici cu privire la gestionarea crizelor, evitând, în același timp, dublarea inutilă a eforturilor în cazul în care necesitățile se suprapun, cu respectarea pe deplin a politicii UE în materie de exerciții și a principiilor incluziunii, reciprocității și autonomiei decizionale a UE;

59. RECUNOAȘTE că Convenția Consiliului Europei privind criminalitatea informatică – Convenția de la Budapesta – oferă un standard juridic eficient care să inspire legislația națională în domeniul criminalității cibernetice. INVITĂ toate țările să elaboreze cadre juridice naționale adecvate și să aibă în vedere cooperarea în acest cadru internațional existent oferit de Convenția de la Budapesta;

60. REAMINTEȘTE rezultatele obținute în urma desfășurării unor dialoguri bilaterale la nivelul UE în domeniul cibernetic și solicită depunerea de eforturi suplimentare pentru facilitarea cooperării cu țările terțe în domeniul securității cibernetice;

61. REAMINTEȘTE că UE dispune de un mecanism de control al exporturilor solid și obligatoriu din punct de vedere juridic, întemeiat pe deciziile și bunele practici dezvoltate în cadrul regimurilor internaționale de neproliferare, și IA ACT de discuțiile în curs de desfășurare în cadrul Consiliului menite să identifice cele mai bune modalități de a îmbunătăți în continuare funcționarea acestor controale și INVITĂ statele membre să continue să abordeze, în cadrul regimu*rilor* internaționale relevante de control al exporturilor (de exemplu Aranjamentul de la Wassenaar), aplicațiile esențiale în domeniul securității cibernetice ale noilor tehnologii, în vederea asigurării unui control eficace al tehnologiilor critice din viitor din domeniul securității cibernetice;

62. Ca urmare a concluziilor Consiliului European din 19 octombrie 2017[21], prezentele concluzii vor fi puse în aplicare prin intermediul unui plan de acțiune care urmează să fie adoptat de către Consiliu înainte de sfârșitul anului 2017. Planul de acțiune ca document evolutiv ar urma să fie revizuit și actualizat periodic de către Consiliu.

---

[21] Doc. EUCO 14/17.