Consiliul
Uniunii Europene

Bruxelles, 20 octombrie 2021
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	19 octombrie 2021
Destinatar:	Delegațiile
Nr. doc. ant.:	12534/21
Subiect:	Concluziile Consiliului cu privire la explorarea potențialului inițiativei privind unitatea cibernetică comună, în completarea răspunsului coordonat al UE la incidentele și crizele de securitate cibernetică de mare amploare – Concluziile Consiliului, 19 octombrie 2021

În anexă, se pun la dispoziția delegațiilor Concluziile Consiliului cu privire la explorarea potențialului inițiativei privind unitatea cibernetică comună, în completarea răspunsului coordonat al UE la incidentele și crizele de securitate cibernetică de mare amploare, astfel cum au fost adoptate de Consiliu în cadrul reuniunii sale din 19 octombrie 2021.

ANEXĂ

Concluziile Consiliului cu privire la explorarea potențialului inițiativei privind unitatea cibernetică comună, în completarea răspunsului coordonat al UE la incidentele și crizele de securitate cibernetică de mare amploare

CONSILIUL UNIUNII EUROPENE,

AMINTIND:

– concluziile sale privind Strategia de securitate cibernetică a UE pentru deceniul digital[1],

– concluziile sale privind răspunsul coordonat al UE la incidentele și crizele de securitate cibernetică de mare amploare[2],

– concluziile sale privind diplomația cibernetică[3],

– concluziile sale privind un cadru privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare („Setul de instrumente pentru diplomația cibernetică”)[4],

– concluziile sale privind securitatea și apărarea[5],

– Un cadru politic de apărare cibernetică al UE[6],

– concluziile sale privind conturarea viitorului digital al Europei[7],

– 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,

---

1 7290/21.
2 10086/18.
3 6122/15 + COR 1.
4 10474/17.
5 8396/21.
6 15585/14.
7 8711/20.

– concluziile sale privind comunicarea comună către Parlamentul European și Consiliu intitulată: „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”[8],

– concluziile sale privind consolidarea capacităților și a capabilităților în domeniul securității cibernetice în UE[9],

1. SUBLINIAZĂ importanța securității cibernetice pentru construirea unei Europe reziliente, digitale și verzi. SUBLINIAZĂ că securitatea cibernetică este indispensabilă pentru prosperitatea și securitatea UE și ale statelor sale membre, ale cetățenilor, ale întreprinderilor și ale instituțiilor sale, precum și pentru susținerea integrității societăților noastre libere și democratice.

2. RECUNOAȘTE caracterul transfrontalier și transsectorial al multor amenințări la adresa securității cibernetice, precum și riscurile și implicațiile potențiale ale campaniilor necontenite de activități cibernetice răuvoitoare, cu un impact mai mare, mai sofisticate, cu țintă mai precisă, mai complexe, mai persistente și/sau mai larg răspândite[10]. Pandemia de COVID-19 a scos în evidență și mai mult vulnerabilitățile societăților noastre și potențialul incidentelor cibernetice de mare amploare de a cauza daune la adresa economiei, a democrației, a serviciilor esențiale și a infrastructurii critice, în special în sectorul sănătății. De asemenea, aceasta a sporit importanța conectivității și dependența societății de rețele și sisteme informatice fiabile, de încredere și sigure. În cele din urmă, pandemia a evidențiat necesitatea unui internet mondial, deschis, liber, stabil și sigur, precum și a încrederii în produsele, procesele și serviciile din domeniul tehnologiei informației și comunicațiilor (TIC), precum și în securitatea acestora, inclusiv necesitatea de a asigura un lanț de aprovizionare rezilient.

---

8 14435/17 + COR 1.
9 7737/19.
10 Raportul ENISA privind situația amenințărilor în 2020.

3. REITEREAZĂ importanța rezilienței cibernetice și a dezvoltării în continuare a cadrului UE de gestionare a crizelor în materie de securitate cibernetică[11] având drept obiectiv un răspuns eficient și în timp util la nivelul UE la incidentele și crizele de securitate cibernetică de mare amploare, precum și integrarea într-o mai mare măsură a acestuia în mecanismele orizontale și sectoriale existente ale UE de răspuns la situații de criză. SUBLINIAZĂ rolul Consiliului și al mecanismului integrat pentru un răspuns politic la crize în asigurarea coordonării și a răspunsului în timp util la nivelul politic al Uniunii în cazul crizelor care au un impact amplu sau o semnificație politică largă, indiferent dacă provin din interiorul sau din afara Uniunii. RELIEFEAZĂ importanța testării unor astfel de cadre și mecanisme în cadrul unor exerciții periodice.

4. AMINTEȘTE că activitățile la nivelul UE în ceea ce privește incidentele și crizele cibernetice de mare amploare au loc în conformitate cu principiile subsidiarității, proporționalității, complementarității, neduplicării și confidențialității. REITEREAZĂ faptul că statele membre dețin responsabilitatea principală pentru răspunsul la incidentele și crizele de securitate cibernetică de mare amploare care le afectează. AMINTEȘTE importanța respectării competențelor statelor membre și a responsabilității exclusive a acestora pentru securitatea națională, în conformitate cu articolul 4 alineatul (2) din Tratatul privind Uniunea Europeană, inclusiv în domeniul securității cibernetice.

5. AMINTEȘTE, în același timp, importanța respectării competențelor și a mandatelor instituțiilor, organelor și agențiilor UE. Înaltul Reprezentant, Comisia și alte instituții, organe și agenții ale UE au, de asemenea, un rol esențial, care decurge din dreptul Uniunii, inclusiv ca urmare a posibilului impact al incidentelor și crizelor de securitate cibernetică de mare amploare asupra pieței unice, precum și asupra funcționării instituțiilor, organelor și agențiilor UE.

[11] 10086/18.

6. SUBLINIAZĂ necesitatea de a se evita suprapunerile inutile și de a se urmări complementaritatea și valoarea adăugată în dezvoltarea în continuare a cadrului UE de gestionare a crizelor în materie de securitate cibernetică, precum și de a se asigura alinierea la mecanismele, inițiativele, rețelele, procesele și procedurile existente la nivel național și european. EVIDENȚIAZĂ importanța raționalizării proceselor și structurilor existente pentru a se reduce complexitatea și, în interesul coeziunii în Uniune, pentru a se îmbunătăți accesibilitatea și capacitatea de răspuns pentru cei care solicită asistență și solidaritate.

7. RECUNOAȘTE aplicabilitatea dreptului internațional, inclusiv a Cartei Organizației Națiunilor Unite în ansamblul său, a dreptului internațional umanitar și a dreptului internațional al drepturilor omului în spațiul cibernetic și PROMOVEAZĂ aderarea la normele, regulile și principiile privind comportamentul responsabil al statelor în spațiul cibernetic, voluntare și fără caracter obligatoriu, aprobate de toate statele membre ale ONU.

8. SALUTĂ progresele înregistrate în ultimii ani în cadrul Consiliului, în special în cadrul Grupului de lucru orizontal pentru chestiuni cibernetice și al altor grupuri de lucru relevante ale Consiliului, precum și în ceea ce privește crearea altor inițiative, rețele și mecanisme de cooperare și de schimb de informații între statele membre, în special a Grupului de cooperare NIS și a rețelei CSIRT, instituite prin Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016, a Rețelei organizațiilor de legătură în materie de crize cibernetice (CyCLONe), precum și în legătură cu proiectele relevante legate de apărarea cibernetică lansate în cadrul cooperării structurate permanente (PESCO)[12], Grupul operativ comun de acțiune împotriva criminalității informatice (J-CAT), Rețeaua judiciară europeană de combatere a criminalității informatice (EJCN), contribuțiile voluntare ale statelor membre la INTCEN UE, precum și coordonarea și cooperarea în contextul setului de instrumente pentru diplomația cibernetică.

[12] În special, „Echipele de răspuns rapid în domeniul cibernetic și asistența reciprocă în ceea ce privește securitatea cibernetică” coordonate de Lituania, „Centrul de coordonare în domeniul cibernetic și informațional”, coordonat de Germania, „Platforma pentru schimbul de informații privind răspunsul la amenințările și incidentele cibernetice”, coordonată de Grecia.

9. AMINTEȘTE cadrele existente de cooperare între instituțiile, organele și agențiile UE, cum ar fi cooperarea structurată dintre ENISA și CERT-UE și Memorandumul de înțelegere dintre ENISA, Agenția Europeană de Apărare (AEA), Centrul european de combatere a criminalității informatice (EC3) al Europolului și CERT-UE. SUBLINIAZĂ importanța continuării schimbului periodic de informații cu Consiliul cu privire la evoluțiile viitoare ale acestor cadre de cooperare.

10. SUBLINIAZĂ importanța consolidării cooperării și a schimbului de informații între diferitele comunități cibernetice din cadrul UE și al statelor sale membre la toate nivelurile necesare – tehnic, operațional și strategic/politic – și a conectării mecanismelor, rețelelor, structurilor, proceselor și procedurilor existente de gestionare a crizelor, în cazul în care acest lucru sprijină și îmbunătățește gestionarea incidentelor și a crizelor cibernetice de mare amploare.

11. RECUNOAȘTE progresele înregistrate de un grup de state membre în ceea ce privește crearea unei capacități cibernetice operaționale comune, „echipele de răspuns rapid în domeniul cibernetic” în cadrul PESCO, cu scopul de a aprofunda cooperarea voluntară în domeniul cibernetic prin asistență reciprocă, inclusiv ca răspuns la incidentele și crizele cibernetice de mare amploare.

12. RECUNOAȘTE experiența și capacitatea permanentă de răspuns a comunității de aplicare a legii în domeniul cooperării operaționale și al schimbului securizat de informații împotriva atacurilor cibernetice transfrontaliere majore prin intermediul Protocolului UE privind răspunsul în situații de urgență al autorităților de aplicare a legii.

13. RECUNOAȘTE punerea în aplicare neîntreruptă a cadrului privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare („setul de instrumente pentru diplomația cibernetică”). AMINTEȘTE că fiecare stat membru este liber să ia, de la caz la caz, propria decizie suverană cu privire la atribuirea unei activități cibernetice răuvoitoare. AMINTEȘTE că măsurile luate în contextul cadrului privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare ar trebui să se bazeze pe o conștientizare comună a situației, convenită între statele membre. INTCEN UE joacă un rol central în calitate de nucleu însărcinat cu furnizarea către UE de elemente de conștientizare a situației și de evaluări ale amenințărilor în domeniul cibernetic, pe baza contribuțiilor voluntare în materie de informații ale statelor membre și fără a aduce atingere competențelor acestora.

14. REITEREAZĂ importanța asistenței reciproce și a solidarității, în conformitate cu articolul 42 alineatul (7) din Tratatul privind Uniunea Europeană și cu articolul 222 din Tratatul privind funcționarea Uniunii Europene, și SOLICITĂ exerciții suplimentare cu o dimensiune cibernetică. AMINTEȘTE necesitatea de a reflecta asupra corelării cadrului UE de gestionare a crizelor în materie de securitate cibernetică cu setul de instrumente pentru diplomația cibernetică și cu dispozițiile articolelor menționate mai sus în cazul unui incident sau al unei crize cibernetice de mare amploare. AMINTEȘTE, de asemenea, că obligațiile statelor membre care decurg din articolul 42 alineatul (7) din Tratatul privind Uniunea Europeană nu aduc atingere caracterului specific al politicii de securitate și apărare a anumitor state membre. AMINTEȘTE totodată că NATO rămâne temelia apărării colective pentru acele state care sunt membre ale acestei organizații.

15. RECUNOAȘTE cooperarea UE-NATO în materie de securitate și apărare cibernetică, inclusiv schimbul de informații dintre CERT-UE și Capacitatea de răspuns la incidente informatice a NATO (NCIRC), cu respectarea deplină a principiilor transparenței, reciprocității și incluziunii, precum și a autonomiei decizionale a ambelor organizații.

16. RECUNOAȘTE importanța cooperării, atunci când este cazul, cu sectorul privat în ceea ce privește exercițiile de schimb de informații și furnizarea de expertiză relevantă, precum și de soluții și servicii de încredere, inclusiv, de exemplu, în ceea ce privește sprijinirea răspunsului la incidente și consolidarea conștientizării situației în rândul diferitelor comunități cibernetice.

17. SUBLINIAZĂ importanța unor canale de comunicare sigure pentru schimbul de informații clasificate și sensibile. EVIDENȚIAZĂ necesitatea unor progrese suplimentare.

În acest sens și ținând seama de cele de mai sus,

18. IA ACT de Recomandarea Comisiei privind crearea unei unități cibernetice comune, ca inițiativă demnă de luat în considerare pentru dezvoltarea în continuare a cadrului UE de gestionare a crizelor în materie de securitate cibernetică[13].

19. INVITĂ UE și statele sale membre să își continue eforturile în direcția unui cadru al UE de gestionare a crizelor în materie de securitate cibernetică mai cuprinzător și mai eficace, pe baza mecanismelor existente și a progreselor deja realizate, și să ia în considerare potențialul inițiativei privind unitatea cibernetică comună de a completa aceste mecanisme prin adoptarea unei abordări etapizate. SUBLINIAZĂ că un proces gradual, transparent și incluziv este esențial pentru consolidarea încrederii și, prin urmare, vital pentru dezvoltarea în continuare a unui cadru al UE de gestionare a crizelor în materie de securitate cibernetică. Acest proces ar trebui să respecte rolurile, competențele și mandatele existente ale statelor membre și ale instituțiilor, organelor și agențiilor UE, precum și principiile enunțate în prezentele concluzii, inclusiv principiile proporționalității, subsidiarității, incluziunii, complementarității, neduplicării și confidențialității informațiilor. SUBLINIAZĂ, în același timp, că orice eventuală participare sau contribuție a statelor membre la o potențială unitate cibernetică comună are un caracter voluntar.

[13] C(2021)4520 final (11155/21 și 11155/21 ADD1).

20. ACCENTUEAZĂ necesitatea stabilirii unor metode de lucru și a unei guvernanțe adecvate, pentru a permite implicarea și participarea tuturor statelor membre la deliberările, la procesul de elaborare și la procesul decizional efectiv cu privire la cadrul UE de gestionare a crizelor în materie de securitate cibernetică, inclusiv cu privire la inițiativa privind potențiala unitate cibernetică comună. SOLICITĂ respectarea prerogativelor Consiliului în temeiul tratatelor și a principiului cooperării loiale.

21. SUBLINIAZĂ importanța identificării și a implicării tuturor comunităților cibernetice relevante din UE și din statele sale membre, ținând seama, în același timp, de diferitele roluri și responsabilități ale acestora în diversele tipuri de incidente și crize cibernetice de mare amploare. SUBLINIAZĂ rolul hotărâtor jucat de Consiliu, în special prin intermediul Grupului de lucru orizontal pentru chestiuni cibernetice, în cadrul elaborării politicilor și al coordonării în ceea ce privește dezvoltarea în continuare a cadrului UE de gestionare a crizelor în materie de securitate cibernetică. INVITĂ, prin urmare, statele membre, Comisia, Serviciul European de Acțiune Externă (SEAE), INTCEN UE, CERT-UE, ENISA, Europolul (EC3), Eurojustul (EJCN), Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC), precum și reprezentanți ai rețelei CSIRT, ai CyCLONe, ai Grupului de cooperare NIS, ai AEA și ai proiectelor PESCO relevante, precum și alte eventuale părți interesate să se implice în acest proces. Ar putea fi explorată mai în profunzime, astfel cum se propune în recomandarea Comisiei, posibilitatea creării unui grup de lucru care să asigure o reprezentare adecvată a tuturor statelor membre și să acționeze sub îndrumarea politică a Consiliului, pentru a servi drept forum temporar care să reunească reprezentanți ai tuturor comunităților cibernetice relevante din statele membre și din cadrul UE. Un astfel de grup de lucru ar trebui să raporteze periodic cu privire la activitățile sale și să prezinte Consiliului eventuale propuneri pentru dezbatere, aprobare și orientări suplimentare. În plus, ar putea fi instituite alte forme de dialog în cadrul comunităților și între acestea, inclusiv prin ateliere, seminare, activități de formare și exerciții comune.

22. SUBLINIAZĂ rolul Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC) și al Rețelei de centre naționale de coordonare în ceea ce privește potențiala unitate cibernetică comună, în special având în vedere rolul acesteia din urmă de a spori în mod substanțial capacitățile tehnologice, soluțiile tehnologice, capabilitățile și competențele Uniunii în domeniul securității cibernetice.

23. INVITĂ UE și statele sale membre să colaboreze în vederea dezvoltării în continuare a cadrului UE de gestionare a crizelor în materie de securitate cibernetică, inclusiv prin explorarea potențialului inițiativei privind o unitate cibernetică comună, prin stabilirea și definirea procesului, inclusiv a etapelor și a calendarului, precum și prin clarificarea obiectivelor și a posibilelor roluri și responsabilități. EVIDENȚIAZĂ necesitatea de a se consolida, în mod prioritar, rețelele și interacțiunile existente în cadrul fiecărei comunități, precum și de a se efectua o inventariere detaliată a posibilelor lacune și nevoi în materie de schimb de informații în cadrul comunităților cibernetice și între acestea, precum și în cadrul instituțiilor, organelor și agențiilor europene și între acestea și, ulterior, de a se conveni asupra posibilelor obiective și priorități principale ale unei potențiale unități cibernetice comune. Fără a aduce atingere rezultatului, SUBLINIAZĂ necesitatea de a se concentra asupra identificării nevoilor în materie de schimb de informații pentru a se ajunge la o conștientizare comună a situației în rândul tuturor comunităților relevante. În identificarea lacunelor și a nevoilor în materie de schimb de informații, inclusiv în ceea ce privește posibila utilizare a platformelor virtuale, ar trebui să se acorde în continuare atenția cuvenită canalelor de comunicare securizate pentru schimbul de informații clasificate și sensibile, SUBLINIIND totodată importanța utilizării infrastructurii deja existente. Introducerea unei abordări treptate este menită să consolideze încrederea și să constituie o bază pentru posibile măsuri suplimentare legate de îmbunătățirea gradului de pregătire și a cooperării operaționale. RECUNOAȘTE că diversele obiective ar putea necesita soluții diverse și implicarea unor grupuri diverse de reprezentanți ai comunităților cibernetice relevante din UE și din statele sale membre.

24. SOLICITĂ o analiză mai detaliată a unui temei juridic pentru potențiala unitate cibernetică comună pe parcursul întregului proces, inclusiv o evaluare a sarcinilor și a rolurilor în raport cu cele atribuite ENISA în recomandare prin prisma articolului 7 din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019. SOLICITĂ o reflecție sporită cu privire la elementele individuale ale Recomandării privind crearea unei unități cibernetice comune, inclusiv în ceea ce privește ideea echipelor UE de reacție rapidă în materie de securitate cibernetică și planul UE de răspuns la incidente și crize de securitate cibernetică. EVIDENȚIAZĂ că o potențială unitate cibernetică comună trebuie să respecte competențele generale, mandatele și competențele juridice ale eventualilor săi viitori participanți.

25. INVITĂ UE și statele sale membre să studieze potențialul inițiativei privind o unitate cibernetică comună, inclusiv din perspectiva instituțiilor, organelor și agențiilor UE, pentru a completa eforturile depuse în prezent la nivelul statelor membre. SALUTĂ intenția Comisiei de a consolida reziliența instituțiilor, organelor și agențiilor relevante ale UE prin intermediul viitoarei sale propuneri de regulament privind normele comune obligatorii în materie de securitate cibernetică pentru instituțiile, organele și agențiile UE.

26. În concluzie, REITEREAZĂ angajamentul său de a consolida reziliența cibernetică și de a dezvolta în continuare cadrul UE de gestionare a crizelor în materie de securitate cibernetică și VA MONITORIZA PERIODIC progresele înregistrate și va oferi orientări suplimentare pentru completarea cadrului UE de gestionare a crizelor în materie de securitate cibernetică.