Consiliul
Uniunii Europene

Bruxelles, 17 octombrie 2022
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	17 octombrie 2022
Destinatar:	Delegațiile
Nr. doc. ant.:	12930/22
Subiect:	Concluziile Consiliului privind securitatea lanțurilor de aprovizionare TIC – Concluzii ale Consiliului aprobate de Consiliu în cadrul reuniunii sale din 17 octombrie 2022

În anexă, se pun la dispoziția delegațiilor Concluziile Consiliului privind securitatea lanțurilor de aprovizionare TIC, astfel cum au fost aprobate de Consiliu în cadrul reuniunii sale desfășurate la 17 octombrie 2022.

ANEXĂ

Concluziile Consiliului privind securitatea lanțurilor de aprovizionare TIC

CONSILIUL UNIUNII EUROPENE,

AMINTIND concluziile sale privind

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

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

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

– conturarea viitorului digital al Europei,

– „o redresare în vederea promovării tranziției către o industrie europeană mai dinamică, rezilientă și competitivă”,

– securitatea cibernetică a dispozitivelor conectate,

– Strategia de securitate cibernetică a UE pentru deceniul digital,

– dezvoltarea poziției cibernetice a Uniunii Europene,

– Raportul special 03/2022 al Curții de Conturi Europene, intitulat „Implementarea tehnologiei 5G în UE: întârzieri în instalarea rețelelor și probleme de securitate încă nerezolvate”,

AMINTIND concluziile Consiliului European privind

– COVID-19, piața unică, politica industrială, dimensiunea digitală și relațiile externe din 1-2 octombrie 2020,

– agresiunea militară rusă împotriva Ucrainei, securitatea și apărarea, energia, aspectele economice, pandemia de COVID-19 și relațiile externe din 24-25 martie 2022,

– Ucraina, securitatea alimentară, securitatea și apărarea și energia din 30-31 mai 2022,

1. având în vedere relevanța tot mai mare a geopoliticii pentru securitatea cibernetică, SUBLINIAZĂ că Uniunea Europeană și statele sale membre trebuie să abordeze securitatea cibernetică într-un mod cuprinzător și strategic. Agresiunea militară a Rusiei împotriva Ucrainei a provocat o schimbare majoră în mediul strategic și de securitate al Uniunii Europene și a demonstrat necesitatea unei Uniuni Europene mai puternice și mai capabile în domeniul securității și apărării. Aceasta a pus în evidență faptul că este extrem de important să se ia în considerare în mod corespunzător mediul geopolitic nu numai atunci când se reacționează la activități cibernetice răuvoitoare, ci și atunci când se construiește și se menține reziliența tehnologiilor informației și comunicațiilor (TIC). Acest lucru este deosebit de relevant pentru lanțurile de aprovizionare cu produse și servicii TIC (lanțuri de aprovizionare TIC), care ar putea fi atât compromise din cauza rivalității geopolitice, după cum o ilustrează atacul SolarWinds, cât și afectate de instabilitate și tensiuni geopolitice, după cum o demonstrează amenințarea legată de dependența de furnizorii ruși de TIC în momentul agresiunii militare a Rusiei împotriva Ucrainei.

2. IA ACT de faptul că natura riscurilor asociate lanțului de aprovizionare TIC, care este alcătuit dintr-un set corelat de resurse și procese între operatorii economici [astfel cum sunt definiți în Regulamentul (UE) 2019/1020] care începe cu aprovizionarea cu materii prime și se extinde prin fabricarea, prelucrarea, gestionarea și livrarea de produse și servicii TIC, inclusiv furnizarea de sprijin pe parcursul ciclului de viață al produselor și serviciilor TIC, generează provocări unice și consecințe care pot fi de amploare. Pe lângă riscurile legate de indisponibilitatea produselor TIC, de exemplu din cauza deficitului de materii prime critice și de semiconductori necesari pentru producția lor, lanțurile de aprovizionare cu produse și servicii TIC sunt expuse și altor amenințări. În special, acestea pot fi vizate sau utilizate în mod abuziv de către actori răuvoitori în moduri sofisticate, adesea ascunse, care au un impact asupra confidențialității, integrității și disponibilității datelor sensibile transmise și stocate.

3. Recunoscând că este necesară o abordare care să țină seama de toate riscurile în ceea ce privește securizarea activelor TIC, RECUNOAȘTE relevanța propunerii de directivă privind reziliența entităților critice pentru a îmbunătăți securitatea fizică a entităților critice și SUBLINIAZĂ că, pe lângă consolidarea rezilienței la atacurile asupra lanțurilor de aprovizionare desfășurate prin mijloace cibernetice, este la fel de important să se consolideze securitatea și reziliența generală a lanțurilor de aprovizionare TIC împotriva întregii varietăți de factori de amenințare, cum ar fi evenimentele naturale, disfuncționalitățile sistemului, amenințările interne sau erorile umane. În acest sens, RECUNOAȘTE că securitatea lanțurilor de aprovizionare TIC presupune asigurarea protecției produselor și serviciilor TIC realizate, furnizate, achiziționate și utilizate în lanțurile de aprovizionare TIC, inclusiv prin protejarea componentelor individuale și a datelor transmise.

4. Bazându-se pe învățămintele desprinse din consecințele dependențelor strategice ale Uniunii Europene de combustibilii fosili ruși, precum și din impactul perturbărilor lanțurilor de aprovizionare în timpul pandemiei de COVID-19, în special în ceea ce privește produsele farmaceutice și semiconductorii, sectoare în care au fost expuse dependențele strategice ale UE, ÎNCURAJEAZĂ statele membre să depună eforturi pentru a evita situații similare de dependențe externe strategice nedorite în ceea ce privește produsele și serviciile TIC. Având în vedere digitalizarea tot mai mare a societății și utilizarea tot mai frecventă a TIC în infrastructura critică, dependențele externe strategice legate de produsele și serviciile TIC și de lanțurile de aprovizionare cu acestea ar trebui evaluate în permanență și, după caz, abordate.

5. AMINTEȘTE că realizarea autonomiei strategice, menținând în același timp o economie deschisă, este un obiectiv-cheie al Uniunii, care include identificarea și reducerea dependențelor strategice și creșterea rezilienței în ecosistemele industriale cele mai sensibile și în domenii specifice, inclusiv în domeniul digital. Aceasta include dezvoltarea și implementarea unor infrastructuri și capacități digitale strategice, precum și consolidarea capacității de a face alegeri tehnologice autonome și – unul dintre pilonii principali – asigurarea unor infrastructuri, produse și servicii reziliente și securizate pentru consolidarea încrederii pe piața unică digitală și în cadrul societății europene, menținând în același timp deschiderea, cooperarea globală cu parteneri care împărtășesc aceeași viziune și competitivitatea și valorificând potențialele beneficii ale acestora. Valorile fundamentale ale Uniunii Europene susțin în mod special viața privată, securitatea, egalitatea, demnitatea umană, statul de drept și internetul deschis drept condiții prealabile pentru realizarea unei societăți, a unei economii și a unei industrii centrate pe factorul uman și având drept vector domeniul digital.

6. IA ACT de faptul că, având în vedere evoluțiile peisajului amenințărilor cibernetice demonstrate de tendința unor atacuri sofisticate și de mare impact asupra lanțurilor de aprovizionare în ultimii ani, cum ar fi atacurile SolarWinds, Mimecast sau Kaseya, care au apărut odată cu externalizarea serviciilor TIC esențiale și care s-au intensificat din cauza dependenței generale de produsele și serviciile TIC realizate, furnizate sau asigurate de părți terțe, este foarte probabil ca în viitor să apară mai multe atacuri asupra lanțurilor de aprovizionare, cu daune substanțiale pentru economie și societate. Ținând seama de acestea, SUBLINIAZĂ importanța sporirii securității și rezilienței lanțurilor de aprovizionare TIC pentru funcționarea pieței unice, precum și necesitatea de a asigura disponibilitatea, securitatea și diversitatea produselor și serviciilor TIC pe piața unică. Prin urmare, RECUNOAȘTE necesitatea de a maximiza și de a raționaliza utilizarea instrumentelor și abordărilor existente ale UE pentru atingerea acestor obiective, precum și necesitatea de a se adapta în permanență la peisajul în schimbare al amenințărilor cibernetice prin introducerea unor măsuri și mecanisme suplimentare adecvate, inclusiv în ceea ce privește posibile riscuri de securitate ale tehnologiilor emergente și disruptive. ÎNCURAJEAZĂ statele membre să urmărească, în acest sens, abordarea bazată pe riscuri pentru a trata noile evoluții tehnologice.

7. RECUNOAȘTE că înțelegerea peisajului amenințărilor cibernetice aflat în continuă evoluție, precum și a complexității atacurilor asupra lanțurilor de aprovizionare este esențială pentru atenuarea eficace a riscurilor asociate lanțurilor de aprovizionare TIC. În acest sens, SUBLINIAZĂ necesitatea de a se adapta la noi amenințări prin monitorizarea, analiza și evaluarea activă și continuă a peisajului amenințărilor asupra lanțurilor de aprovizionare, de a crește gradul de conștientizare și de a consolida cunoștințele cu privire la amenințări și vulnerabilități, precum și de a alerta în mod proactiv entitățile relevante într-un mod adaptat. SALUTĂ activitatea Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) în ceea ce privește securitatea lanțurilor de aprovizionare TIC, în special raportul său privind peisajul amenințărilor pentru atacurile asupra lanțurilor de aprovizionare.

INSTRUMENTE ȘI ABORDĂRI TRANSSECTORIALE

8. REAFIRMĂ că este important ca statele membre să ia în considerare necesitatea de a diversifica furnizorii de TIC critice pentru a evita sau a limita crearea unor dependențe majore de furnizori unici, în special furnizorii cu grad ridicat de risc, deoarece aceasta sporește expunerea la consecințele unor potențiale perturbări. RECUNOAȘTE că evitarea dependenței de furnizori și diversificarea furnizorilor TIC reprezintă una dintre componentele importante pentru asigurarea stabilității și securității pieței interne. SUBLINIAZĂ necesitatea de a promova și de a pune în aplicare strategii adecvate care să faciliteze diversificarea și competitivitatea furnizorilor într-un mod neutru din punct de vedere tehnologic. În plus, ÎNCURAJEAZĂ integrarea aspectelor legate de prevenirea dependenței de furnizori în legislația UE. În acest sens, IA ACT de propunerea de regulament privind norme armonizate pentru un acces echitabil la date și o utilizare corectă a acestora (Legea privind datele), care urmărește să sporească interoperabilitatea serviciilor de prelucrare a datelor și să elimine obstacolele din calea trecerii de la un furnizor de servicii de prelucrare a datelor la altul.

9. RECUNOAȘTE legătura dintre securitatea lanțurilor de aprovizionare TIC și achizițiile publice. SUBLINIAZĂ necesitatea ca procedurile de achiziții publice să țină seama în mod adecvat de importanța securității lanțurilor de aprovizionare TIC prin impunerea, după caz, a unor criterii de selecție obiective și bazate pe riscuri legate de capacitatea ofertanților de a asigura un nivel ridicat de securitate a serviciilor furnizate. SOLICITĂ găsirea unui echilibru adecvat între interesul public pentru cea mai eficientă și echitabilă utilizare a fondurilor publice, pe de o parte, și interesul public în ceea ce privește securizarea sistemelor de informații și asigurarea bunei funcționări a pieței unice, pe de altă parte. Pentru a facilita punerea în aplicare a normelor relevante privind achizițiile publice în contextul creșterii securității cibernetice, INVITĂ Comisia să elaboreze orientări metodologice până în al treilea trimestru al anului 2023 pentru a încuraja autoritățile contractante să pună accentul în mod corespunzător pe practicile în materie de securitate cibernetică ale ofertanților și ale subcontractanților acestora și să evalueze legislația relevantă privind achizițiile publice și, dacă este necesar, să facă propuneri de revizuire sau completare a acestei legislații.

10. RECUNOAȘTE că investițiile străine directe legate de produsele și serviciile TIC, deși oferă beneficii economice și sociale statelor membre, întreprinderilor și cetățenilor, ar putea include riscuri la adresa securității și a ordinii publice și IA ACT de faptul că mecanismul de examinare a investițiilor străine directe al UE, alături de diferitele sisteme naționale de examinare, care oferă mijloace de abordare a acestor riscuri, ar putea fi, de asemenea, aplicate ca instrument util pentru asigurarea securității și a rezilienței lanțurilor de aprovizionare TIC, contribuind la eliminarea investițiilor cu grad ridicat de risc care pot afecta securitatea și reziliența lanțurilor respective. RECUNOAȘTE că informațiile partajate prin intermediul acestui mecanism pot ajuta statele membre să evalueze mai bine posibilele amenințări la adresa securității lanțurilor de aprovizionare TIC și să ia măsurile necesare în consecință. INVITĂ actorii naționali relevanți să țină seama, de asemenea, de această dimensiune a mecanismului de examinare, după caz.

11. În ceea ce privește apărarea, REAFIRMĂ invitația adresată Comisiei de a evalua, în 2023, împreună cu statele membre, riscurile pentru lanțurile de aprovizionare cu infrastructuri critice din diferite domenii, inclusiv domeniul digital, legate de interesele UE în materie de securitate și apărare, precum și de a examina opțiuni de creștere a securității cibernetice de-a lungul întregului lanț de aprovizionare al bazei industriale și tehnologice de apărare a UE. În plus, INVITĂ statele membre și Comisia să reflecteze asupra securității lanțurilor de aprovizionare TIC în punerea în aplicare a angajamentelor și acțiunilor Busolei strategice.

12. Recunoscând importanța materiilor prime critice, precum și a tuturor tipurilor de semiconductori ca elemente constitutive de bază pentru produsele TIC, ÎNCURAJEAZĂ negocieri constructive asupra propunerii de regulament de stabilire a unui cadru de măsuri pentru consolidarea ecosistemului european al semiconductorilor (Actul privind cipurile) și a propunerii de regulament al Consiliului de modificare a Regulamentului (UE) 2021/2085 de instituire a întreprinderilor comune din cadrul programului Orizont Europa, în ceea ce privește întreprinderea comună pentru cipuri.

INSTRUMENTE SPECIFICE DOMENIULUI CIBERNETIC

13. În special în ceea ce privește infrastructura de telecomunicații, RECUNOAȘTE realizările obținute la nivelul Uniunii cu privire la îmbunătățirea securității lanțului de aprovizionare al rețelelor 5G, mai ales prin intermediul setului de instrumente al UE pentru securitatea rețelelor 5G (setul de instrumente al UE pentru 5G). INVITĂ statele membre să facă în continuare schimb de informații în materie de bune practici și metodologii privind punerea în aplicare a măsurilor recomandate în setul de instrumente al UE pentru 5G și, în special, să aplice restricțiile relevante asupra furnizorilor cu grad ridicat de risc pentru activele-cheie definite drept critice și sensibile în evaluarea coordonată a riscurilor la nivelul UE. SUBLINIAZĂ că setul de instrumente al UE pentru 5G reprezintă un instrument flexibil, bazat pe riscuri, pentru abordarea provocărilor în materie de securitate identificate, care permite gestionarea aspectelor legate de securitatea cibernetică a rețelelor 5G în timp util și în mod eficient, cu respectarea competențele statelor membre și RECUNOAȘTE că acesta este un instrument valoros pentru a consolida în continuare, în deplină transparență, securitatea lanțului de aprovizionare al rețelelor de telecomunicații într-un mod coordonat, un instrument care ar putea servi drept sursă de inspirație pentru instrumentele de evaluare și atenuare a riscurilor aferente altor sectoare vitale. AMINTEȘTE invitația autorităților relevante de a formula recomandări, bazate pe evaluări ale riscurilor, adresate statelor membre și Comisiei pentru a consolida reziliența rețelelor și a infrastructurilor de comunicații în cadrul Uniunii Europene, inclusiv în ceea ce privește continuarea punerii în aplicare a setului de instrumente al UE pentru 5G.

14. IA ACT de importanța abordărilor interoperabile care pot soluționa dependența de furnizori și pot atenua riscul de concentrare, îmbunătățind în același timp securitatea lanțurilor de aprovizionare în întregul spectru al infrastructurii și serviciilor TIC. În special în ceea ce privește rețelele 5G, RECUNOAȘTE în acest sens beneficiile potențiale ale conceptului privind o rețea de acces radio (RAN) deschisă, AMINTEȘTE totodată Raportul privind securitatea cibernetică a RAN deschise publicat de Grupul de cooperare NIS, în care se constată că acest concept este încă în curs de dezvoltare și că securitatea, transparența și standardizarea sa sunt într-o fază incipientă și SUBLINIAZĂ importanța evaluării riscurilor înaintea oricărei tranziții către noi standarde sau arhitecturi.

15. SUBLINIAZĂ relevanța instrumentelor legislative orizontale existente și viitoare în materie de securitate cibernetică, în special a Regulamentului privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor (Regulamentul privind securitatea cibernetică), a viitoarei Directive privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS 2), a propunerii de regulament privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii, precum și a propunerii de regulament privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale (Actul privind reziliența cibernetică), pentru creșterea securității lanțurilor de aprovizionare TIC. În plus, IA ACT de evoluțiile importante înregistrate la nivelul reglementărilor sectoriale în materie de securitate cibernetică, în special în ceea ce privește viitorul Regulament privind reziliența operațională digitală a sectorului financiar (DORA), care include un cadru de supraveghere pentru furnizorii terți de servicii TIC care sunt esențiali pentru entitățile financiare. Aceste reglementări prevăd obligații generale legate de securitatea lanțurilor de aprovizionare, precum și cerințe detaliate și specifice relevante pentru sectorul în cauză. În același timp, ACCENTUEAZĂ faptul că, adesea, furnizorii își furnizează produsele și își prestează serviciile în mai multe sectoare, mai degrabă decât într-un singur sector. Prin urmare, este extrem de important să se asigure că cerințele privind securitatea lanțurilor de aprovizionare sunt, în măsura posibilului, aliniate în toate sectoarele relevante, în special în cele vizate de viitoarea Directivă NIS 2, pentru a se evita discrepanțele dintre obligațiile impuse furnizorilor, precum și pentru a se ușura sarcina operatorilor din sectoarele critice de a evalua respectarea acestor obligații de către furnizori, ținându-se seama, în același timp, de particularitățile fiecărui sector.

16. SALUTĂ propunerea de act privind reziliența cibernetică drept un instrument legislativ important pentru înregistrarea de progrese în ceea ce privește dezvoltarea în condiții de securitate a produselor cu elemente digitale și pentru asigurarea faptului că securitatea cibernetică este luată în considerare pe parcursul întregului ciclu de viață al produselor cu elemente digitale. REMARCĂ faptul că propunerea de act privind reziliența cibernetică are potențialul de a contribui în mod semnificativ la consolidarea securității lanțurilor de aprovizionare TIC. ÎNCURAJEAZĂ negocierile constructive și adoptarea actului în timp util.

17. În această privință, RECUNOAȘTE activitatea în curs condusă de ENISA, împreună cu statele membre și cu alte părți interesate, pentru a furniza UE sisteme de certificare pentru produsele, serviciile și procesele TIC conforme cu Regulamentul privind securitatea cibernetică, care ar trebui să contribuie la sporirea nivelului general de securitate cibernetică în cadrul pieței unice digitale. ÎNCURAJEAZĂ toate părțile interesate să participe la lucrările pregătitoare privind sistemele europene de certificare individuale pentru a întări încrederea în produse, procese și servicii TIC securizate și pentru a consolida reziliența acestora și SOLICITĂ Comisiei ca, după finalizarea lucrărilor pregătitoare, să elaboreze rapid acte de punere în aplicare privind sistemele europene de certificare, în special sistemul european de certificare a securității cibernetice bazat pe criterii comune (EUCC). REMARCĂ faptul că sistemele europene de certificare ar trebui să includă, acolo unde este necesar, cerințe privind securitatea lanțurilor de aprovizionare, inclusiv în ceea ce privește relațiile cu furnizorii.

18. SUBLINIAZĂ necesitatea punerii în aplicare cu rigurozitate a tuturor dispozițiilor din cadrul viitoarei Directive NIS 2 care se referă la securitatea lanțurilor de aprovizionare TIC. În acest sens, SUBLINIAZĂ relevanța evaluărilor coordonate la nivelul UE ale riscurilor din cadrul lanțurilor de aprovizionare critice (evaluări coordonate ale riscurilor din cadrul lanțurilor de aprovizionare), a politicilor naționale în materie de securitate a lanțurilor de aprovizionare și a măsurilor de securitate legate de lanțurile de aprovizionare. REMARCĂ faptul că, în ceea ce privește riscurile la adresa securității furnizorului primar sau a clientului final, ar trebui să se acorde atenție nu numai furnizorilor primari, ci și subcontractanților relevanți. Pentru a facilita punerea în aplicare a măsurilor de gestionare a riscurilor din cadrul lanțurilor de aprovizionare, ÎNCURAJEAZĂ ENISA să realizeze, cu sprijinul Grupului de cooperare NIS, un bilanț al bunelor practici disponibile pentru gestionarea riscurilor din cadrul lanțurilor de aprovizionare și să le compileze în orientări metodologice. În plus, ÎNCURAJEAZĂ ENISA să monitorizeze investițiile în securitatea lanțurilor de aprovizionare TIC ale entităților reglementate de viitoarea Directivă NIS 2.

19. EVIDENȚIAZĂ, de asemenea, beneficiile și riscurile utilizării unor furnizori de servicii gestionate (MSP) și a unor furnizori de servicii de securitate gestionate (MSSP) în contextul securității lanțurilor de aprovizionare. Deși utilizarea acestor furnizori poate îmbunătăți în mod semnificativ securitatea în cadrul organizațiilor și poate conduce la niveluri mai ridicate de securitate cibernetică, gestionarea la distanță a sistemelor și serviciilor TIC, combinată cu un acces privilegiat la mediul TIC al clienților, de care ar putea avea nevoie MSP și MSSP, poate genera, în cazul unor MSP și MSSP compromiși, efecte în cascadă cu impact asupra unui număr mare de clienți. Prin urmare, este extrem de important ca MSP și MSSP să mențină un nivel ridicat de securitate internă proprie și de securitate a serviciilor pe care le furnizează și să adopte o abordare transparentă față de clienții lor în ceea ce privește securitatea serviciilor pe care le furnizează. În acest sens, SALUTĂ faptul că MSP și MSSP vor fi incluși în domeniul de aplicare al viitoarei Directive NIS 2.

20. În ceea ce privește punerea în aplicare a mecanismului de evaluare coordonată a riscurilor din cadrul lanțurilor de aprovizionare în temeiul viitoarei Directive NIS 2, IA ACT de importanța în acest context a factorilor de risc fără caracter tehnic, cum ar fi influența nejustificată a unui stat terț asupra furnizorilor și prestatorilor de servicii și, în acest context, RECUNOAȘTE relevanța factorilor care pot fi utilizați pentru evaluarea profilului de risc, astfel cum se menționează în evaluarea coordonată la nivelul UE a riscurilor legate de securitatea cibernetică a rețelelor 5G. INVITĂ Comisia să identifice, până în al doilea trimestru al anului 2023, după consultarea Grupului de cooperare NIS și a ENISA, serviciile, sistemele sau produsele TIC specifice care ar putea fi supuse cu prioritate evaluărilor coordonate ale riscurilor din cadrul lanțurilor de aprovizionare.

21. IA ACT de faptul că dependențele de furnizori cu grad ridicat de risc de produse și servicii TIC utilizate pentru funcționarea rețelelor și sistemelor critice reprezintă o amenințare strategică care trebuie atenuată prin politici adecvate atât la nivel național, cât și la nivelul UE și prin cooperare între statele membre și cu parteneri internaționali care împărtășesc aceeași viziune. Pentru a facilita atenuarea acestui risc strategic și pentru a sprijini evaluările coordonate ale riscurilor din cadrul lanțurilor de aprovizionare, INVITĂ Grupul de cooperare NIS, în cooperare cu Comisia și ENISA, să elaboreze un set de măsuri pentru reducerea riscurilor critice din cadrul lanțurilor de aprovizionare TIC (setul de instrumente pentru lanțurile de aprovizionare TIC). Setul de instrumente pentru lanțurile de aprovizionare TIC ar trebui să se bazeze pe scenariile de amenințare strategică identificate pentru lanțurile de aprovizionare TIC și să prevadă măsuri pentru a răspunde acestor scenarii, valorificând cunoștințele obținute pe baza setului de instrumente pentru 5G și experiența dobândită la nivel național. Acesta ar trebui să completeze, în mod transparent, evaluările coordonate ale riscurilor din cadrul lanțurilor de aprovizionare pentru servicii, sisteme sau produse TIC specifice în temeiul viitoarei Directive NIS 2, oferind măsuri generice de reducere a riscurilor care pot fi ajustate, la o scară mai mare sau mai mică, pentru servicii, sisteme sau produse TIC specifice, pe baza riscurilor identificate în evaluările individuale coordonate ale riscurilor din cadrul lanțurilor de aprovizionare.

22. ACCENTUEAZĂ rolul important al cercetării, inovării, investițiilor și activităților antreprenoriale în domeniul digital și al securității cibernetice, precum și rolul finanțării unor astfel de activități, în vederea evitării pe viitor a unor eventuale dependențe strategice nedorite și a consolidării rezilienței generale a lanțurilor de aprovizionare TIC. În acest context, SUBLINIAZĂ că atât sarcinile strategice, cât și sarcinile de punere în aplicare ce revin Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC) și Rețelei de centre naționale de coordonare au un rol și o importanță deosebite, contribuind la maximizarea efectelor investițiilor pentru a consolida poziția de lider și autonomia strategică deschisă ale Uniunii în domeniul securității cibernetice, pentru a sprijini capacitățile și competențele tehnologice ale Uniunii și pentru a spori competitivitatea Uniunii la nivel mondial. În acest sens, SOLICITĂ operaționalizarea rapidă a ECCC. Invită ECCC să ia în considerare, în agenda sa strategică, aspectele legate de securitatea lanțurilor de aprovizionare TIC, inclusiv, de exemplu, dezvoltarea de software securizat, asigurând, în același timp, coerența și complementaritatea și evitând orice suprapunere a eforturilor. SPRIJINĂ consolidarea competitivității europene în domeniul securității cibernetice prin programe de finanțare, cum ar fi programul-cadru pentru cercetare și inovare Orizont Europa, precum și programul Europa digitală pentru consolidarea, construirea și achiziționarea de capacități esențiale pentru economia digitală a UE, pentru societate și democrație.

MECANISME DE SPRIJIN

23. ÎNCURAJEAZĂ sporirea stimulentelor sub formă de sprijin financiar aferente măsurilor care vizează consolidarea securității lanțurilor de aprovizionare TIC. SOLICITĂ Comisiei și părților interesate relevante ca, inclusiv în vederea viitoarei puneri în aplicare a Directivei NIS 2, în ceea ce privește ECCC, să examineze în mod prioritar opțiuni pentru includerea aspectelor legate de securitatea lanțurilor de aprovizionare TIC în cererile de propuneri care vor fi lansate în contextul programelor de lucru în materie de securitate cibernetică din cadrul programului Europa digitală și al programului Orizont Europa sau orice alte oportunități de finanțare relevante. Unul dintre obiectivele acestor oportunități de finanțare ar trebui să fie acela de a permite organizațiilor să sprijine menținerea unui nivel ridicat de securitate cibernetică în ceea ce privește achiziționarea de produse și servicii TIC de-a lungul întregului lanț de aprovizionare, în special în raport cu înlocuirea unor servicii, sisteme sau produse TIC critice specifice, recunoscute, în conformitate cu viitoarele evaluări coordonate ale riscurilor din cadrul lanțurilor de aprovizionare, ca prezentând un grad ridicat de risc.

24. RECUNOAȘTE că globalizarea și specializarea serviciilor TIC, precum și dependența sporită de produse și servicii ale unor terți implică necesitatea unei cooperări strânse în cadrul UE și la nivel internațional în ceea ce privește schimbul de cunoștințe și expertiză între părțile interesate relevante și ÎNCURAJEAZĂ aceste părți interesate să adopte o poziție solidă și coordonată care să asigure securitatea lanțurilor de aprovizionare TIC într-un mod cuprinzător. RECUNOAȘTE, de asemenea, necesitatea de a explora în continuare abordări și tehnici de ultimă generație relevante, atât pentru o igienă cibernetică de bază adecvată, cât și pentru soluții pe termen lung în vederea realizării unor lanțuri de aprovizionare TIC securizate și reziliente, precum și cele mai adecvate modalități de promovare și de includere potențială a acestora în politici sau în alte inițiative. RECUNOAȘTE, în acest sens, că ar trebui să se acorde o atenție deosebită examinării beneficiilor și dezavantajelor unor soluții sistematice, cum ar fi principiile „încredere zero” sau lista de componente ale software-ului, precum și ale altor soluții similare pe termen lung. RECOMANDĂ utilizarea Grupului de cooperare NIS în acest scop.

25. IA ACT de beneficiile monitorizării incidentelor și amenințărilor cibernetice și ale schimbului eficace de informații cu privire la acestea pentru prevenirea, depistarea și atenuarea efectelor atacurilor asupra lanțurilor de aprovizionare. SUBLINIAZĂ necesitatea de a se continua consolidarea încrederii între statele membre în vederea unui schimb eficace de astfel de informații. AMINTEȘTE în această privință 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 atacuri asupra rețelelor. AMINTEȘTE că este nevoie de complementaritate și coordonare în cadrul rețelelor și mecanismelor existente și, în acest sens, SUBLINIAZĂ în special rolul rețelei echipelor de intervenție în caz de incidente de securitate informatică (CSIRT) și necesitatea de a examina în continuare potențialul acestei rețele de a promova o cultură a unui schimb de informații eficient, securizat și fiabil. AMINTEȘTE eforturile depuse de statele membre, sprijinite de UE, pentru a institui CSIRT-uri 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.

26. Având în vedere caracterul interconectat și global al amenințărilor asupra lanțurilor de aprovizionare TIC, EVIDENȚIAZĂ importanța abordării și consolidării securității lanțurilor de aprovizionare TIC la nivel mondial. Ținând seama de acest lucru, RECOMANDĂ utilizarea parteneriatelor digitale, a dialogurilor pe teme cibernetice și a altor inițiative relevante ale UE, inclusiv, după caz, a acordurilor de liber schimb, pentru promovarea evaluărilor bazate pe riscuri ale furnizorilor de produse TIC și ale prestatorilor de servicii TIC, pentru utilizarea unor furnizori de încredere și pentru implementarea unui ecosistem digital securizat și inovator, bazat pe standarde deschise, interoperabile și transparente. În plus, REITEREAZĂ viziunea parteneriatelor din cadrul Global Gateway și a Consiliului UE-SUA pentru comerț și tehnologie, precum și activitățile desfășurate de grupurile de lucru ale acestui Consiliu, pentru a promova utilizarea unor furnizori de încredere/care nu prezintă un grad ridicat de risc și pentru a dezvolta un mecanism de finanțare a proiectelor care contribuie la sporirea nivelului de securitate și reziliență a infrastructurii și serviciilor TIC din statele terțe, precum și la sporirea nivelului de încredere față de acestea, inclusiv prin nefinanțarea unor achiziții de la furnizori care nu sunt de încredere/care prezintă un grad ridicat de risc, într-un mod neutru din punct de vedere tehnologic.

27. ÎȘI REAFIRMĂ angajamentul de a contribui la un spațiu cibernetic deschis, liber, global, stabil și securizat și de a-l promova, precum și de a adera la normele, regulile și principiile comportamentului responsabil al statelor în spațiul cibernetic prevăzute în cadrul ONU. În special în ceea ce privește securitatea lanțurilor de aprovizionare TIC, AMINTEȘTE norma aprobată de grupul de experți guvernamentali (GEG) al ONU și de grupul de lucru deschis (OEWG) care încurajează statele să ia măsuri rezonabile pentru a asigura integritatea lanțurilor de aprovizionare, inclusiv prin elaborarea unor măsuri de cooperare obiective, astfel încât utilizatorii finali să poată avea încredere în securitatea produselor TIC, și să urmărească să prevină proliferarea instrumentelor și tehnicilor TIC răuvoitoare și utilizarea funcțiilor ascunse dăunătoare și PLEDEAZĂ pentru punerea în aplicare a acestei norme pe scară largă.