Vijeće
Europske unije

Bruxelles, 20. studenoga 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

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Na datum:	20. studenoga 2017.
Za:	Delegacije
Br. preth. dok.:	13943/17 + COR 1
Br. dok. Kom.:	12210/17, 12211/17
Predmet:	Zaključci Vijeća o Zajedničkoj komunikaciji Europskom parlamentu i Vijeću: Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a – zaključci Vijeća (20. studenoga 2017.)

Za delegacije se u prilogu nalaze zaključci Vijeća o Zajedničkoj komunikaciji Europskom parlamentu i Vijeću: Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a, koje je Vijeće za opće poslove usvojilo 20. studenoga 2017.

PRILOG

Zaključci Vijeća o Zajedničkoj komunikaciji Europskom parlamentu i Vijeću: Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a

Vijeće Europske unije,

1. PREPOZNAJUĆI važnost kibersigurnosti za blagostanje, rast i sigurnost EU-a te cjelovitost naših slobodnih i demokratskih društava i njihovih temeljnih procesa u digitalnom dobu, i putem zaštite vladavine prava i zaštite ljudskih prava i temeljnih sloboda svakog pojedinca;

2. ISTIČUĆI potrebu da se za kibersigurnost razvije dosljedan pristup na nacionalnoj razini, razini EU-a te globalnoj razini, s obzirom na to da kiberprijetnje mogu utjecati na našu demokraciju, blagostanje, stabilnost i sigurnost;

3. NAPOMINJE da je visoka razina kiberotpornosti diljem EU-a važna i za izgradnju povjerenja u jedinstveno digitalno tržište te daljnji razvoj digitalne Europe;

4. PONOVNO ISTIČUĆI da će EU stalno promicati otvoren, globalan, slobodan, miroljubiv i siguran kiberprostor, u kojem se i u EU-u i na globalnoj razini potpuno primjenjuju i poštuju ljudska prava i temeljne slobode, pogotovo pravo na slobodu izražavanja, pristup informacijama, zaštitu podataka, privatnost i sigurnost te temeljne vrijednosti i načela EU-a te NAGLAŠAVAJUĆI ključnu važnost osiguravanja odgovarajuće ravnoteže između ljudskih prava i temeljnih sloboda te potreba politike unutarnje sigurnosti EU-a[1],

5. PREPOZNAJUĆI činjenicu da se međunarodno pravo, među ostalim Povelja UN-a u cjelini, međunarodno humanitarno pravo i pravo o ljudskim pravima primjenjuju u kiberprostoru te stoga NAGLAŠAVAJUĆI potrebu za daljnjim ulaganjem napora kako bi se osiguralo da se međunarodno pravo poštuje u kiberprostoru;

[1] 12650/17.

6. PODSJEĆAJUĆI NA zaključke o strategiji Europske unije za sigurnost kibernetičkog prostora[2], o upravljanju Internetom[3], o jačanju kiberotpornosti EU-a[4], o kibernetičkoj diplomaciji[5] te o okviru za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti[6], o unapređenju kaznenog pravosuđa u kiberprostoru[7]; o sigurnosti i obrani u okviru globalne strategije EU-a[8], Zajednički okvir za suzbijanje hibridnih prijetnji[9], te o preispitivanju obnovljene strategije unutarnje sigurnosti Europske unije za razdoblje 2015. – 2020. u sredini programskog razdoblja[10];

7. PREPOZNAJUĆI da se okvirom uspostavljenim Konvencijom Vijeća Europe o kibernetičkom kriminalu (Konvencija iz Budimpešte) raznolikoj skupini zemalja osigurava čvrst temelj za upotrebu učinkovitog pravnog standarda za različita nacionalna zakonodavstva i za međunarodnu suradnju u borbi protiv kiberkriminaliteta;

8. PREPOZNAJUĆI potrebu za ponovnim stavljanjem težišta na provedbu okvira za politiku kibernetičke obrane EU-a za 2014. i za njegovim ažuriranjem kako bi se u Zajedničku sigurnosnu i obrambenu politiku (ZSOP) dodatno integrirali kibersigurnost i obrana te za širim programom sigurnosti i obrane;

9. PREPOZNAJUĆI da je globalno konkurentna europska industrija važan element za postizanje visoke razine kibersigurnosti na nacionalnoj razini i diljem EU-a;

10. PODSJEĆAJUĆI da je u skladu s člankom 4. stavkom 2. UEU-a nacionalna sigurnost isključiva odgovornost svake države članice.

---

2 Dok. 12109/13 i dok. 6225/13 (Zajednička komunikacija Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija: Strategija Europske unije za sigurnost kibernetičkog prostora: otvoren, siguran i zaštićen kibernetički prostor (COM JOIN (2013) 1 final).

3 Dok. 16200/14 i dok. 6460/14 (Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija: Politika interneta i upravljanje internetom: Uloga Europe u oblikovanju budućnosti upravljanja internetom (COM (2014) 72 final).

4 Dok. 14540/16 i dok. 11013/16 (Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija: Jačanje europskog sustava kibernetičke sigurnosti i poticanje konkurentne i inovativne industrije kibernetičke sigurnosti (COM 2016(410) final).

5 6122/15.

6 9916/17.

7 10007/16.

8 9178/17.

9 7688/16 (Zajednička komunikacija Europskom parlamentu i Vijeću: Zajednički okvir za suzbijanje hibridnih prijetnji – odgovor Europske unije).

10 12650/17.

OVIME

11. POZDRAVLJA činjenicu da se Zajedničkom komunikacijom Europskom parlamentu i Vijeću pod naslovom: „Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a” postavlja ambiciozan cilj poboljšanja kibersigurnosti unutar EU-a. Njome se također doprinosi strateškoj autonomiji EU-a, kako je navedeno u Zaključcima Vijeća o globalnoj strategiji Europske unije za vanjsku i sigurnosnu politiku[11], i to izgradnjom digitalne Europe koja će biti sigurnija, svjesnija svoje snage, konkurentnija, otvorenija svijetu, koja će graditi veće povjerenje te još više poštovati zajedničke vrijednosti EU-a u pogledu otvorenog, slobodnog, miroljubivog i sigurnog globalnog interneta, te stoga postiže viša razina otpornosti kako bi se spriječilo i otkrilo kiberprijetnje, odvratilo od njih i reagiralo na njih te kako bi se moglo zajednički odgovoriti na kiberprijetnje diljem EU-a te

12. POZIVA države članice te institucije, agencije i tijela EU-a da surađuju, uzajamno poštujući područja nadležnosti i načela supsidijarnosti i proporcionalnosti kao odgovor na strateške ciljeve utvrđene u navedenim zaključcima te

13. ISTIČE da je potrebno da EU, njegove države članice i privatni sektor osiguraju dostatna financijska sredstva, u okviru dostupnih sredstava, za podršku izgradnji kiberotpornosti te naporima u istraživanju i razvoju u području kibersigurnosti diljem EU-a, kao i za jačanje suradnje kako bi se spriječilo i otkrilo kiberprijetnje, odvratilo od njih i reagiralo na njih te kako bi se moglo zajednički odgovoriti na kiberincidente velikih razmjera i zlonamjerne kiberaktivnosti diljem EU-a;

[11] 13202/16.

Poglavlje I.

OSIGURAVANJE UČINKOVITE KIBEROTPORNOSTI EU-a I POVJERENJA U JEDINSTVENO DIGITALNO TRŽIŠTE

14. NAGLAŠAVA da je svaka država članica prvenstveno odgovorna za svoju kibersigurnost i osiguravanje svojeg odgovora na kiberincidente i kiberkrize, dok EU može pružiti veliku dodanu vrijednost u podupiranju suradnje među državama članicama. U tom kontekstu, ISTIČE potrebu da sve države članice stave potrebna sredstva na raspolaganje nacionalnim tijelima odgovornima za kibersigurnost kako bi se osigurali sprečavanje, identifikacija i odgovaranje na kiberincidente i kiberkrize diljem EU-a;

15. NAGLAŠAVA potrebu da se po mogućnosti upotrebljavaju postojeći mehanizmi, strukture i organizacije na razini EU-a;

16. POHVALJUJE:

- napredak koji su države članice postigle u prenošenju Direktive o mrežnoj i informacijskoj sigurnosti u nacionalno pravo te ISTIČE potrebu za postizanjem pune i učinkovite provedbe do svibnja 2018., kako je propisano u toj Direktivi[12];
- napore koje je skupina za suradnju u području mrežne i informacijske sigurnosti uložila u jačanje strateške suradnje i razmjene informacija među državama članicama;
- rad koji je obavila mreža timova za odgovor na računalne sigurnosne incidente (CSIRT), posebno u jačanju operativne suradnje država članica, izgradnji povjerenja i pouzdanja u razmjenu informacija prilikom rješavanja opsežnih incidenata u području kibersigurnosti te, na temelju nacionalnih zaključaka država članica, u osiguravanju elemenata za zajednički uvid u stanje na razini Europe;
- rad obavljen u okviru ugovornog javno-privatnog partnerstva u području kibersigurnosti (cPPP).

[12] Ne dovodeći u pitanje nadležnost država članica za prenošenje Direktive o mrežnoj i informacijskoj sigurnosti u nacionalno pravo, posebno u pogledu operatorâ ključnih usluga.

17. POZDRAVLJA činjenicu da je u Zajedničkoj komunikaciji potvrđeno da je snažno i pouzdano šifriranje iznimno važno kako bi se na odgovarajući način osigurala ljudska prava i temeljne slobode u EU-u i za javno povjerenje u jedinstveno digitalno tržište, ali i da se istodobno uzima u obzir da tijela za izvršavanje zakonodavstva trebaju imati pristup podacima nužnima za njihove istrage te da je potvrđeno da su sigurna digitalna identifikacija i komunikacija ključne u osiguravanju učinkovite kibersigurnosti u EU-u;

18. POZDRAVLJA plan u Zajedničkoj komunikaciji o većim ambicijama u pogledu redovite provedbe paneuropskih vježbi u području kibersigurnosti, na temelju iskustva stečenog u vježbama „Cyber Europe", kojima se kombiniraju odgovori na različitim razinama, jer će to biti važan element u povećanju spremnosti država članica i institucija EU-a u odgovaranju na kiberincidente velikih razmjera;

19. POZIVA EU i njegove države članice da provode redovne strateške vježbe u području kibersigurnosti u različitim sastavima Vijeća, na temelju iskustva stečenog u vježbama EU CYBRID 2017. te

20. Ne dovodeći u pitanje ishod zakonodavnog postupka:

- POZDRAVLJA prijedlog za snažan i trajan mandat ENISA-e, čiji je glavni cilj podupirati i razvijati užu suradnju među državama članicama, povećavati njihove kapacitete i povećati povjerenje u digitalnu Europe;

- PONOVNO POTVRĐUJE da bi se buduća Europska agencija za mrežnu i informacijsku sigurnost (ENISA) trebala osloniti na iskustvo i stručnost unutar država članica i EU-a te podupirati neprekidan razvoj i provedbu postojećih i budućih politika i propisa EU-a u području kibersigurnosti, te bi se trebalo osigurati da se sve nadležnosti ENISA-e razvijaju kao dopuna nadležnosti država članica;

- PONOVNO POTVRĐUJE cilj jačanja pouzdanja u digitalnu Europu povećanjem povjerenja i pouzdanja u digitalna rješenja i inovacije, među ostalim „internet stvari”, e-trgovinu i e-upravljanje, posebno u pogledu prvoklasnog europskog okvira za kibersigurnosnu certifikaciju[13]. To je ključan preduvjet za povećanje povjerenja i sigurnosti u području digitalnih proizvoda i usluga, zaštitu ključne infrastrukture, podataka državnih tijela, podataka građana i poslovnih podataka te presudno za usvajanje pristupa integrirane sigurnosti za proizvode, usluge i procese na jedinstvenom digitalnom tržištu;

- ISTIČE da će se zakonodavnim radom na jačanju certifikacije kibersigurnosti na razini EU-a morati zadovoljiti potrebe tržišta i korisnikâ, da će se morati temeljiti na iskustvima u području postojećih kapacitetâ i procesa certifikacije u EU-u (npr. okvira Skupine viših dužnosnika za sigurnost informacijskih sustava (SOG-IS)) te da bi se njime morao osigurati okvir sposoban za brzu prilagodbu na najsuvremenije buduće digitalne trendove;

- ISTIČE da je prilikom poboljšanja certifikacije kibersigurnosti u EU-u potrebno obuhvatiti čitav spektar sigurnosnih zahtjeva, od najmanjih do najvećih, kada se mora dokazati otpornost na sposobnosti napadača. Ključan čimbenik za uspjeh jest osiguravanje pouzdanog, transparentnog i neovisnog procesa za sigurnosnu certifikaciju u svrhu promicanja dostupnosti pouzdanih i sigurnih uređaja, softvera i usluga na jedinstvenom tržištu i izvan njega; prepoznajući stručnost europske industrije, vlada i stručnjaka za evaluaciju putem odgovarajućih europskih i svjetskih standarda[14]; poštujući ulogu država članica u postupku certifikacije, posebno u pogledu evaluacije na višim sigurnosnim razinama i u odnosu na procjenu ključnih sigurnosnih potreba i vještina. Takvim okvirom za certifikaciju trebalo bi osigurati i da je svaki sustav certifikacije na razini EU-a proporcionalan razini sigurnosti potrebne za uporabu dotičnih proizvoda, usluga i/ili sustava informacijskih i komunikacijskih tehnologija, te da se njime omogućuje prekogranično trgovanje za poduzeća svih veličina kako bi razvijala i prodavala nove proizvode, i unutar EU-a i izvan tržištâ EU-a.

---

13 Primjenom globalnih standarda razvijenih u duhu Kodeksa o dobroj praksi iz Sporazuma WTO-a o tehničkim preprekama u trgovini.

14 Primjenom europskih i globalnih standarda razvijenih u duhu Kodeksa o dobroj praksi iz Sporazuma WTO-a o tehničkim preprekama u trgovini.

21. POZDRAVLJA namjeru uspostave mreže centara za stručnost u području kibersigurnosti radi poticanja razvoja i primjene tehnologija u području kibersigurnosti i dodatnog poticanja inovacija za industriju EU-a na globalnoj razini u razvoju tehnologija sljedeće generacije i revolucionarnih tehnologija, kao što su umjetna inteligencija, kvantno računalstvo, ulančani blokovi (*blockchain*) i sigurni digitalni identiteti;

22. ISTIČE da je potrebno da mreža centara za stručnost u području kibersigurnosti bude uključiva prema svim državama članicama i njihovim postojećim centrima za izvrsnost i stručnost te posveti posebnu pažnju na komplementarnost i s tim na umu PRIMA NA ZNANJE planirani europski centar za kibersigurnost i istraživanje, čija bi ključna uloga bila osiguravanje komplementarnosti i izbjegavanje preklapanja unutar mreže centara za stručnost u području kibersigurnosti te s drugim agencijama EU-a;

23. ISTIČE da bi se mreža centara za stručnost u području kibersigurnosti trebala baviti nizom pitanja, od istraživanja do industrije te bi stoga među ostalim trebala doprinositi postizanju cilja europske strateške autonomije;

24. S obzirom na predloženu mrežu centara za stručnost u području kibersigurnosti PONOVNO POTVRĐUJE potrebu da EU putem svojih država članica razvija europski kapacitet za evaluaciju snage kriptografije koja se upotrebljava u proizvodima i uslugama za građane, poduzeća i vlade u okviru jedinstvenog digitalnog tržišta, iako prima na znanje da su politike za kriptografiju ključni aspekt nacionalne sigurnosti te su stoga u nadležnosti država članica;

25. POZIVA sve relevantne dionike da povećaju ulaganja u primjenu novih tehnologija u području kibersigurnosti kako bi se doprinijelo osiguravanju kibersigurnosti u svim sektorima europskog gospodarstva;

26. NAGLAŠAVA važnost vjerodostojnog, pouzdanog i koordiniranog pružanja kibersigurnosnih usluga institucijama EU-a i POZIVA KOMISIJU i druge institucije EU-a da u skladu s tim ciljevima dodatno unaprijede tim CERT-EU te ujedno za to osiguraju odgovarajuća sredstva;

27. POZDRAVLJA poziv na uvažavanje važne uloge koju istraživači trećih strana koji se bave pitanjima sigurnosti imaju u otkrivanju ranjivosti postojećih proizvoda i usluga te POZIVA države članice da razmjenjuju najbolju praksu za koordinirano otkrivanje ranjivosti;

28. NAGLAŠAVA da smo za kibersigurnost odgovorni svi i POZIVA EU i njegove države članice da promiču digitalne vještine i medijsku pismenost čime se korisnicima pomaže da zaštite svoje digitalne podatke na internetu i podiže razina svijesti o opasnostima unošenja osobnih podataka na internetu;

29. POZDRAVLJA stavljanje naglaska na obrazovanje, kiberhigijenu i osviještenost u državama članicama i EU-u u okviru zajedničke komunikacije;

30. POZIVA KOMISIJU da brzo provede procjenu učinka i do sredine 2018. predloži relevantni pravni instrument za provedbu inicijative za uspostavu mreže centara za stručnost u području kibersigurnosti i Europskog centra za istraživanje i stručnost u području kibersigurnosti;

31. POZIVA države članice da:

- u informativnim kampanjama stave naglasak na osvješćivanje u pogledu kibersigurnosti i potiču kibersigurnost u programima akademskog obrazovanja i strukovnog osposobljavanja. Trebalo bi se posebno usmjeriti na obrazovanje mladih i promicanje digitalnih vještina kako bi se osposobili stručnjaci koji se mogu suočiti s budućim promjenama i spremni su na izazove u području sigurnosti, gospodarstvu i uslugama;

- pojačaju napore u pokretanju specijaliziranih programa za kibersigurnost na visokoj razini kako bi se riješio trenutačni manjak stručnjaka u području kibersigurnosti u EU-u:

- uspostave djelotvornu mrežu za suradnju kontaktnih točaka za obrazovanje u okviru ENISA-e. Mreža kontaktnih točaka za cilj bi trebala imati poboljšati koordinaciju i razmjenu najbolje prakse među državama članicama u vezi s obrazovanjem i podizanjem razine svijesti u području kibersigurnosti, kao i s osposobljavanjem, vježbom i izgradnjom kapaciteta;

- razmotre primjenu pravila Direktive o mrežnoj i informacijskoj sigurnosti i na javne uprave koje sudjeluju u ključnim društvenim ili gospodarskim aktivnostima, ako se na njih već ne primjenjuje nacionalno zakonodavstvo i ako se to smatra potrebnim te da osposobljavanje u području kibersigurnosti omoguće i u javnoj upravi s obzirom na ulogu koju ona ima u našem društvu i gospodarstvu;

Poglavlje II.

IZGRADNJA KAPACITETA EU-a ZA SPREČAVANJE I OTKRIVANJE ZLONAMJERNIH KIBERAKTIVNOSTI, ODVRAĆANJE OD NJIH TE REAGIRANJE NA NJIH

32. NAGLAŠAVA da bi posebno ozbiljan kiberincident ili kiberkriza trebali bi biti dostatna osnova da se država članica pozove na klauzulu solidarnosti EU-a[15] i/ili klauzulu o uzajamnoj pomoći[16];

33. POZDRAVLJA donošenje okvira za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti kojim se doprinosi sprečavanju sukoba, suradnji i stabilnosti u kiberprostoru utvrđivanjem mjera u okviru ZVSP-a koje uključuju mjere ograničavanja i mogu se koristiti za sprečavanje zlonamjernih kiberaktivnosti i reagiranje na njih te POZIVA ESVD i države članice da redovito provode vježbe na temelju tog okvira;

---

[15] Članak 222. UFEU-a.
[16] Članak 42. stavak 7. UEU-a.

34. NAGLAŠAVA potrebu za učinkovitim odgovorom na kiberincidente i kiberkrize velikih razmjera na razini EU-a, uz poštovanje nadležnosti država članica te potrebu da se kibersigurnost uključi u postojeće mehanizme za upravljanje krizama na razini EU-a[17]. Kako bi se to postiglo POZIVA na redovito pružanje odgovora na kiberincidente velikih razmjera na razini EU-a, od diplomatsko-strateških do tehničkih odgovora, na temelju odgovarajućih okvira i procedura te, prema potrebi, poboljšavajući ih[18];

35. NAGLAŠAVA važnost dobro integriranih mehanizama za odgovor i razmjenu informacija među različitim zajednicama koji su ključni za osiguravanje kibersigurnosti u Europi, među ostalim među relevantnim tijelima EU-a i država članica. Takvi mehanizmi trebat će se testirati i provjeriti u okviru vježbi u području kibersigurnosti na razini EU-a i, prema potrebi, formalizirati odgovarajućim dogovorima;

36. PRIMA NA ZNANJE mogućnost ispitivanja, ako ga ona predstavi, Komisijina prijedloga za uspostavu Fonda za hitne kibersigurnosne intervencije uz postojeće napore država članica i poštujući dostupna sredstva (posebno u okviru višegodišnjeg financijskog okvira EU-a) za pomoć državama članicama u odgovoru na kiberincidente velikih razmjera i njihovu sprečavanju, pod uvjetom da je država članica uspostavila razborit kibersigurnosni sustav prije incidenta, među ostalim i da je u potpunosti provela Direktivu o mrežnoj i informacijskoj sigurnosti i razradila okvire za upravljanje krizama i nadzor na nacionalnoj razini;

37. PREPOZNAJE sve čvršće veze između kibersigurnosti i obrane te POZIVA na jačanje suradnje u području kiberobrane, među ostalim potičući suradnju između civilnih i vojnih zajednica za odgovor na incidente, i na nastavak jačanja kibersigurnosti misija i operacija ZSOP-a;

---

17 C/2017/6100 final.
18 9916/17 i C/2017/6100 final.

38. NAGLAŠAVA potrebu da se potencijalno u potpunosti iskoriste predložene obrambene inicijative za ubrzanje razvoja odgovarajućih sposobnosti u području kiberkriminaliteta u Europi i PREPOZNAJE potencijal u mogućoj izradi projekata kiberobrane u okviru stalne strukturirane suradnje, ako države članice koje u njoj sudjeluju to budu smatrale potrebnim te PREPOZNAJE ulogu tehnološke i industrijske baze europske obrane (EDTIB) i šire civilne baze industrije kibersigurnosti u osiguravanju sredstava za zaštitne mjere država članica u odnosu na njihove interese obrane i sigurnosti u vezi sa kiberkriminalitetom;

39. PRIMA NA ZNANJE prijedlog Komisije za uspostavu platforme za obrazovanje i osposobljavanje u području kiberobrane do kraja 2018. i NAGLAŠAVA da bi se platformom trebalo unaprijediti mogućnosti osposobljavanja i obrazovanja u okviru država članica te osigurati komplementarnost s drugim naporima i inicijativama EU-a, posebno s EASO-om i EDA-om;

40. POZIVA EU i države članice na reakciju na prijetnju krađe intelektualnog vlasništva potpomognute informatičkim i komunikacijskim tehnologijama, uključujući poslovne tajne ili druge povjerljive poslovne informacije, s namjerom omogućavanja konkurentske prednosti pojedinim poduzećima ili poslovnim sektorima;

41. PREPOZNAJE potrebu za rješavanjem kaznenih djela u kiberprostoru, među ostalim i u mračnom internetu (*Darkweb*), seksualnog iskorištavanja djece na internetu, kao i prijevara i krivotvorenja bezgotovinskih sredstava plaćanja, prije svega poboljšanjem obavještajnog uvida, provođenjem zajedničkih istraga i zajedničkom operativnom potporom;

42. POZDRAVLJA djelovanja EU-a i njegovih država članica u suočavanju s izazovima sustavâ koji kriminalcima i teroristima omogućavaju komunikaciju kojoj nadležna tijela nemaju pristup, NAGLAŠAVA da se tim djelovanjima u obzir mora uzeti da je snažno i pouzdano šifriranje iznimno važno za kibersigurnost i povjerenje u jedinstveno digitalno tržište te osigurati poštovanje ljudskih prava i temeljnih sloboda;

43. ISTIČE važnost toga da se tijelima za izvršavanje zakonodavstva pruže alati kojima bi im bilo omogućeno otkrivanje, istraga i kazneni progon kiberkriminaliteta, kako kaznena djela u kiberprostoru ne bi prošla nezamijećeno ili nekažnjeno te POZDRAVLJA doprinos Europske pravosudne mreže za kiberkriminalitet u borbi protiv kriminaliteta suradnjom pravosudnih tijela;

44. NAGLAŠAVA važnost osiguravanja koordiniranog stajališta EU-a kako bi se unutar zajednice s više interesnih skupina učinkovito formirale odluke o upravljanju internetom u Europi i globalno, npr. kako bi se omogućile brzo dostupne i precizne baze podataka WHOIS-a koje sadrže IP adrese i nazive domena, s ciljem zaštite sposobnosti izvršavanja zakonodavstva i javnih interesa;

45. NAGLAŠAVA važnost uvođenja internetskog protokola IPv6 koji je ključan za razmjerni razvoj „interneta stvari" i lakši pronalazak odgovornih za kaznena djela u kiberprostoru;

46. POTIČE aktualni rad na prekograničnom pristupu elektroničkim dokazima, rješavanju pitanja zadržavanja podataka i na izazovima koje kaznenim postupcima nameću sustavi koji kriminalcima i teroristima omogućavaju komunikaciju kojoj nadležna tijela nemaju pristup, uzimajući u obzir potrebu za poštovanjem ljudskih prava i temeljnih sloboda te zaštitom podataka;

47. POZIVA Komisiju:

- da do prosinca 2017. predstavi izvješće o napretku na temu provedbe praktičnih mjera za poboljšanje prekograničnog pristupa elektroničkim dokazima;
- da početkom 2018. predstavi zakonodavni prijedlog za poboljšanje prekograničnog pristupa elektroničkim dokazima;

48. POZIVA Europol, ENISA-u i Eurojust:

- da nastave jačati svoju suradnju u borbi protiv kiberkriminaliteta, i međusobno i s drugim relevantnim dionicima, među ostalim zajednicom CSIRT-ova, Interpolom, privatnim sektorom i akademskom zajednicom, uz osiguravanje sinergija i komplementarnosti te u skladu s njihovim mandatima i nadležnostima;

- da zajedno s državama članicama doprinose koordiniranom pristupu za odgovor tijela za izvršavanje zakonodavstva EU-a na kiberincidente i kiberkrize velikih razmjera kako bi se nadopunile procedure navedene u relevantnim okvirima[19];

49. POZIVA EU i njegove države članice da nastave rad:

- na uklanjanju prepreka u istraživanju kriminala i učinkovitom kaznenom pravosuđu za kiberprostor, kao i na poboljšanju međunarodne suradnje i koordinacije u borbi protiv kriminala u kiberprostoru;

- na rješavanju izazova nametnutih tehnologijom za anonimizaciju, uzimajući u obzir da je snažno i pouzdano šifriranje iznimno važno za kibersigurnost i povjerenje u jedinstveno digitalno tržište;

- na formiranju odluka o upravljanju internetom, koje utječu na sposobnost tijela za izvršavanje zakonodavstva u borbi protiv kriminala u kiberprostoru;

[19] 9916/17 i C/2017/6100 final.

Poglavlje III.

JAČANJE MEĐUNARODNE SURADNJE ZA OTVOREN, SLOBODAN, MIROLJUBIV I SIGURAN GLOBALNI KIBERPROSTOR

50. PREPOZNAJE da je osiguravanje kibersigurnosti globalan izazov koji zahtjeva učinkovitu globalnu suradnju među svim dionicima te UVIĐA da je poseban naglasak potrebno staviti na pružanje podrške demokratskim vrijednostima i načelima otvorenog, slobodnog, miroljubivog i sigurnog globalnog kiberprostora;

51. POZIVA EU i njegove države članice na promicanje uspostavljanja strateškog okvira za sprečavanje sukoba, suradnju i stabilnosti u kiberprostoru temeljenog na primjeni postojećeg međunarodnog prava, osobito Povelje UN-a u cjelini, razvoju i primjeni univerzalnih normi za odgovorno ponašanje država te regionalnih mjera za izgradnju povjerenja među državama;

52. PREPOZNAJE ulogu Ujedinjenih naroda u dodatnom razvoju normi za odgovorno ponašanje država u kiberprostoru i podsjeća da je raspravama Skupine vladinih stručnjaka u okviru Ujedinjenih naroda tijekom godina postignut konsenzus o nizu normi i preporuka[20] koje je Opća skupština u više navrata poduprla i koje bi države trebale prihvatiti kao temelj za odgovorno ponašanje država u kiberprostoru;

53. PREPOZNAJE da se tim normama odgovornog ponašanja država podrazumijeva da države ne bi trebale svjesno dopustiti da se njihovo državno područje upotrebljava za međunarodne prijestupe, da bi one trebale odgovoriti na odgovarajuće zahtjeve za pomoć druge države čija je ključna infrastruktura pod utjecajem zlonamjernog djelovanja informatičkih i komunikacijskih tehnologija iz njihovog državnog područja te da bi države trebale poduzeti odgovarajuće mjere za zaštitu svoje ključne infrastrukture od prijetnji uzrokovanih informatičkim i komunikacijskim tehnologijama;

54. PREPOZNAJE kiberprijetnje i rizike koji su zajednički EU-u, NATO-u i njihovim državama članicama i PONOVNO ISTIČE važnost nastavka suradnje EU-a i NATO-a u području kibersigurnosti i obrane uz potpuno poštovanje načela uključivosti, reciprociteta i autonomije postupka donošenja odluka u EU-u te u skladu sa svojim zaključcima od 6. prosinca 2016. o provedbi Zajedničke izjave predsjednika Europskog vijeća, predsjednika Europske komisije i glavnog tajnika Organizacije sjevernoatlantskog ugovora[20];

55. POZIVA EU i njegove države članice da podupru i potaknu izradu regionalnih mjera za izgradnju povjerenja, koje su ključni element za veću suradnju i transparentnost te smanjenje rizika od sukoba. Provođenjem mjera za izgradnju povjerenja u kibernetičku sigurnost u okviru OESS-a i drugim regionalnim okvirima povećat će se predvidljivost ponašanja države i dodatno doprinijeti stabilizaciji kiberprostora;

56. POTVRĐUJE da će EU nastaviti podupirati svoje temeljne vrijednosti u zaštiti ljudskih prava i temeljnih sloboda u skladu s EU-ovim smjernicama o ljudskim pravima u odnosu na slobodu na internetu. EU ujedno ističe važnost uključivanja svih dionika u upravljanje internetom, uključujući akademsku zajednicu, civilno društvo i privatni sektor;

57. POZIVA EU i njegove države članice na promicanje jačanja kapaciteta u području kibersigurnosti u trećim zemljama u svrhu rješavanja kiberkriminaliteta i jačanja kiberotpornosti, u skladu s temeljnim vrijednostima EU-a, s tim da prednost imaju zemlje u susjedstvu EU-a i zemlje u razvoju u kojima se brzo povećava povezivost. Za dodatne napore u tom području trebalo bi izraditi mrežu EU-a za jačanje kapaciteta u području kibersigurnosti i smjernice EU-a za jačanje kapaciteta u području kibersigurnosti koje bi trebale biti komplementarne postojećim mehanizmima i strukturama;

[20] 15283/16.

58. ISTIČE napredak ostvaren u suradnji EU-a i NATO-a u području kiberobrane i kibersigurnosti te njezin razvoj u području osposobljavanja. obrazovanja i koncepta uz izbjegavanje nepotrebnog udvostručavanja napora u slučaju preklapanja zahtjevâ, kao i u poticanju interoperabilnosti s pomoću zahtjeva za kibersigurnost, te standarda te POZIVA na nastavak suradnje u vježbama kiberobrane (na razini osoblja) i razmjenu dobre prakse za upravljanje krizama, uz izbjegavanje nepotrebnog udvostručavanja napora u slučaju preklapanja zahtjevâ, poštujući u potpunosti politiku EU-a u području vježbi i načela uključivosti, reciprociteta i autonomije postupka donošenja odluka u EU-u;

59. PREPOZNAJE da se Konvencijom Vijeća Europe o kibernetičkom kriminalu (Konvencija iz Budimpešte) pruža učinkovit pravni standard za obavješćivanje tijela nacionalnog zakonodavstva o kiberkriminalitetu. POZIVA sve države da osmisle odgovarajući nacionalni pravni okvir i nastave suradnju u okviru tog postojećeg međunarodnog okvira zadanog Konvencijom iz Budimpešte;

60. PODSJEĆA na postignuća u provođenju bilateralnih kiberdijalog EU-a i poziva na ulaganje dodatnih napora u olakšanje suradnje s trećim zemljama u području kibersigurnosti;

61. PODSJEĆA da EU ima stabilan i pravno obvezujući mehanizam za kontrolu izvoza koji se temelji na odlukama i najboljoj praksi izrađenima u međunarodnim režimima o neširenju oružja i PRIMA NA ZNANJE rasprave koje su u tijeku u Vijeću kako bi se našli najbolji načini za dodatno poboljšanje funkcioniranja tih kontrola te POZIVA države članice da nastave rješavati, u relevantnim međunarodnim režimima za kontrolu izvoza (npr. Sporazumu iz Wassenaara), ključne primjene novih tehnologija u području kibersigurnosti, kako bi se osigurala djelotvorna kontrola ključnih tehnologija budućnosti u području kibersigurnosti;

62. Kao daljnje postupanje u odnosu na zaključke Europskog vijeća od 19. listopada 2017.[21] ti će se zaključci provoditi putem akcijskog plana koji će Vijeće donijeti do kraja 2017. Akcijski plan Vijeće bi, kao dokument podložan promjenama, redovito preispitivalo i ažuriralo;

---

[21] EUCO 14/17.