Svet
Evropske unije

Bruselj, 20. november 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

IZID POSVETOVANJA

Pošiljatelj:	generalni sekretariat Sveta
Datum:	20. november 2017
Prejemnik:	delegacije
Št. predh. dok.:	13943/17 + COR 1
Št. dok. Kom.:	12210/17, 12211/17
Zadeva:	Sklepi Sveta o Skupnem sporočilu Evropskemu parlamentu in Svetu: Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU – sklepi Sveta (20. november 2017)

V prilogi vam pošiljamo sklepe Sveta o Skupnem sporočilu Evropskemu parlamentu in Svetu z naslovom „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“, ki jih je Svet za splošne zadeve sprejel 20. novembra 2017.

PRILOGA

Osnutek sklepov Sveta o Skupnem sporočilu Evropskemu parlamentu in Svetu: Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU

Svet Evropske unije

1. PRIZNAVA pomen kibernetske varnosti za blaginjo, rast in varnost EU, pa tudi integriteto naših svobodnih in demokratičnih družb ter digitalnodobnih procesov, na katerih stojijo, in sicer z varovanjem tako pravne države in človekovih pravic kot tudi temeljnih svoboščin vsakega posameznika;

2. POSEBEJ POUDARJA, da je potreben koherenten pristop k obravnavi kibernetske varnosti na ravni držav članic, na ravni EU in na globalni ravni, saj lahko kibernetske grožnje vplivajo na našo demokracijo, blaginjo, stabilnost in varnost;

3. UGOTAVLJA, da je visoka raven kibernetske odpornosti po vsej EU pomembna tudi za zaupanje v enotni digitalni trg in za nadaljnji razvoj digitalne Evrope;

4. PONOVNO POUDARJA, da bo EU vztrajno promovirala odprt, globalen, svoboden, miroljuben in varen kibernetski prostor, v katerem se človekove pravice in temeljne svoboščine, zlasti pravica do svobode izražanja, dostopa do informacij, varstva podatkov, zasebnosti in varnosti, pa tudi temeljne vrednote in načela EU tako v EU kot na svetovni ravni dosledno uveljavljajo in spoštujejo, in hkrati POUDARJA, da je ključno zagotoviti ustrezno ravnotežje med človekovimi pravicami in temeljnimi svoboščinami ter izpolnjevanjem zahtev politike EU na področju notranje varnosti[1];

5. PRIZNAVA, da se v kibernetskem prostoru uporabljajo mednarodno pravo, vključno z Ustanovno listino ZN v celoti, mednarodno humanitarno pravo in pravo na področju človekovih pravic, in zato POSEBEJ POUDARJA, da si je treba še naprej prizadevati za zagotavljanje spoštovanja mednarodnega prava v kibernetskem prostoru;

[1] Dok. 12650/17.

6. OPOZARJA NA svoje sklepe o Strategiji EU za kibernetsko varnost[2], o upravljanju interneta[3], krepitvi kibernetske odpornosti EU[4], o kibernetski diplomaciji[5] in o okviru za skupno diplomatsko odzivanje EU na zlonamerne kibernetske dejavnosti[6], o izboljšanju kazenskega pravosodja v kibernetskem prostoru[7], o varnosti in obrambi v okviru globalne strategije EU[8], o skupnem okviru o preprečevanju hibridnih groženj[9] ter o vmesnem pregledu prenovljene strategije notranje varnosti za Evropsko unijo 2015–2020[10];

7. PRIZNAVA, da okvir, ki ga nudi Konvencija Sveta Evrope o kibernetski kriminaliteti (Budimpeška konvencija), predstavlja trdno osnovo, na kateri lahko pisana skupina držav uporabi učinkovit pravni standard za različne nacionalne zakonodaje in za mednarodno sodelovanje na področju preprečevanja kibernetske kriminalitete;

8. PRIZNAVA, da je treba v ospredje ponovno postaviti izvajanje okvira politike EU za kibernetsko obrambo iz leta 2014 in ga posodobiti zaradi nadaljnje vključitve kibernetske varnosti v skupno varnostno in obrambno politiko (SVOP) ter v agendo za varnost in obrambo nasploh;

9. PRIZNAVA, da je globalno konkurenčna evropska industrija pomemben element za doseganje visoke ravni kibernetske varnosti na ravni držav članic in na ravni celotne EU;

10. OPOZARJA, da je v skladu s členom 4(2) PEU nacionalna varnost v izključni pristojnosti vsake od držav članic.

---

2 Dok. 12109/13 in dok. 6225/13 (Skupno sporočilo Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij: Strategija Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor (dok. COM JOIN (2013) 1 final)).

3 Dok. 16200/14 in dok. 6460/14 (Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij: Internetna politika in upravljanje interneta – Vloga Evrope pri oblikovanju prihodnosti upravljanja interneta (dok. COM(2014) 72 final)).

4 Dok. 14540/16 in dok. 11013/16 (Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij: Krepitev odpornosti evropskega sistema kibernetske varnosti ter spodbujanje konkurenčne in inovativne industrije kibernetske varnosti (dok. COM 2016(410) final)).

5 Dok. 6122/15.

6 Dok. 9916/17.

7 Dok. 10007/16.

8 Dok. 9178/17.

9 Dok. 7688/16 (Skupno sporočilo Evropskemu parlamentu in Svetu: Skupni okvir o preprečevanju hibridnih groženj – odziv Evropske unije).

10 Dok. 12650/17.

ZATO

11. POZDRAVLJA Skupno sporočilo Evropskemu parlamentu in Svetu z naslovom „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“, ker je v njem izpostavljen ambiciozen cilj okrepitve kibernetske varnosti v EU. Prav tako prispeva k strateški avtonomiji EU, ki jo omenjajo sklepi Sveta o globalni strategiji za zunanjo in varnostno politiko Evropske unije[11], saj mu gre za izgradnjo digitalne Evrope, ki bo varnejša, ki bo spodbujala zaupanje, ki se bo zavedala svojih prednosti, ki bo konkurenčna, ki bo odprta v svet, ki bo spoštovala skupne vrednote EU na odprtem, svobodnem, miroljubnem in varnem globalnem internetu – in bo torej dosegla višjo raven odpornosti v kontekstu preprečevanja, odvračanja in odkrivanja kibernetskih groženj ter odzivanja nanje, sposobna pa se bo tudi skupaj odzivati na kibernetske grožnje po vsej EU; poleg tega

12. POZIVA države članice ter institucije, agencije in organe EU, naj med seboj sodelujejo in pri tem spoštujejo pristojnosti ter načeli subsidiarnosti in sorazmernosti, v smislu strateških ciljev iz teh sklepov; hkrati pa

13. POSEBEJ POUDARJA, da morajo EU, njene države članice in zasebni sektor zagotoviti zadostno financiranje ob upoštevanju razpoložljivih sredstev za podporo krepitvi kibernetske odpornosti ter prizadevanjem na področju raziskav in razvoja kibernetske varnosti po vsej EU, okrepiti sodelovanje za namene preprečevanja, odvračanja in odkrivanja kibernetskih groženj ter odzivanja nanje ter biti sposobni skupnega odzivanja na kibernetske incidente velikih razsežnosti in zlonamerne kibernetske dejavnosti po vsej EU;

[11] Dok. 13202/16.

Poglavje I

ZAGOTAVLJANJE UČINKOVITE KIBERNETSKE ODPORNOSTI EU IN ZAUPANJA V ENOTNI DIGITALNI TRG

14. POSEBEJ POUDARJA, da ima vsaka država članica primarno odgovornost za krepitev lastne kibernetske varnosti ter za zagotavljanje odzivanja na kibernetske incidente in krize, medtem ko lahko EU zagotavlja visoko dodano vrednost pri podpori sodelovanju med državami članicami. V zvezi s tem POUDARJA, da morajo vse države članice dati na razpolago potrebna sredstva za nacionalne organe, odgovorne za kibernetsko varnost, s katerimi bodo ti zagotavljali preprečevanje in odkrivanje kibernetskih incidentov in kriz ter odzivanje nanje po vsej EU;

15. POSEBEJ POUDARJA, da je treba, kjer je to mogoče, izkoristiti obstoječe mehanizme, strukture in organizacije na ravni EU;

16. POZDRAVLJA:

- napredek, ki so ga države članice dosegle pri prenosu direktive o varnosti omrežij in informacij, in POUDARJA, da se mora dosledno in učinkovito izvajanje začeti najpozneje maja 2018, kot je določeno v navedeni direktivi[12];
- delo, ki je bilo v okviru skupine za sodelovanje glede varnosti omrežij in informacij opravljeno na področjih krepitve strateškega sodelovanja in izmenjave informacij med državami članicami;
- delo, opravljeno v okviru mreže skupin CSIRT, zlasti na področjih krepitve operativnega sodelovanja držav članic, vzpostavitve zaupanja v izmenjavo informacij pri obvladovanju kibernetskih incidentov velikih razsežnosti in, na podlagi nacionalnih ugotovitev držav članic, zagotavljanja elementov za skupno spremljanje razmer na evropski ravni;
- delo, opravljeno v okviru pogodbenega javno-zasebnega partnerstva za kibernetsko varnost;

[12] Brez poseganja v pristojnost držav članic za prenos direktive o varnosti omrežij in informacij, zlasti kar zadeva izvajalce bistvenih storitev.

17. POZDRAVLJA dejstvo, da je v skupnem sporočilu potrjeno ne le, da je močno in zaupanje vlivajoče šifriranje zelo pomembno za ustrezno zagotavljanje človekovih pravic in temeljnih svoboščin v EU ter za zaupanje javnosti v enotni digitalni trg, ob upoštevanju, da morajo imeti organi odkrivanja in pregona dostop do podatkov, potrebnih za svoje preiskave, temveč tudi, da imata varna digitalna identifikacija in komunikacija ključno vlogo pri zagotavljanju učinkovite kibernetske varnosti v EU;

18. POZDRAVLJA v skupnem sporočilu predstavljeni načrt za povečanje ambicij pri rednem izvajanju vseevropskih vaj na področju kibernetske varnosti, izhajajoč iz izkušenj, pridobljenih iz vaj v okviru Cyber Europe, z združevanjem odzivanja na različnih ravneh, saj bo to pomembno pripomoglo k boljši pripravljenosti držav članic in institucij EU za odzivanje na kibernetske incidente velikih razsežnosti;

19. POZIVA EU in njene države članice, naj v različnih sestavah Sveta izvajajo redne strateške vaje iz kibernetske varnosti, pri tem pa se opirajo na izkušnje, pridobljene v okviru vaje EU CYBRID 2017, in hkrati

20. brez poseganja v izid zakonodajnega postopka:

- POZDRAVLJA predlog za trden in trajen mandat agencije ENISA, katerega primarni cilj je podpreti in vzpostaviti tesnejše sodelovanje med državami članicami, okrepiti njihove zmogljivosti ter poglobiti zaupanje v digitalno Evropo, ter

- PONOVNO POTRJUJE, da bi se morala agencija ENISA v prihodnje opirati na izkušnje in strokovno znanje v državah članicah in EU ter podpirati skladen razvoj in dosledno izvajanje sedanjih in prihodnjih politik in predpisov EU na področju kibernetske varnosti, pri tem pa bi bilo treba poskrbeti, da se bodo vse njene pristojnosti razvijale tako, da bodo dopolnjevale pristojnosti držav članic;

- PONOVNO POTRJUJE cilj, da poglobi zaupanje v digitalno Evropo s povečanjem zaupanja v digitalne rešitve in inovacije, vključno z internetom stvari, e-trgovino in e-upravljanjem, zlasti v smislu vrhunskega evropskega certifikacijskega okvira za kibernetsko varnost[13]. To je ključni pogoj za krepitev zaupanja in varnosti na področju digitalnih proizvodov in storitev kot tudi za zaščito kritične infrastrukture ter podatkov vlad, podatkov o državljanih in poslovnih podatkov, hkrati pa ima pomembno vlogo za uporabo pristopa vgrajene varnosti za proizvode, storitve in procese na enotnem digitalnem trgu;

- POUDARJA, da bo moralo zakonodajno delo za krepitev certificiranja na področju kibernetske varnosti na ravni EU zadovoljiti potrebe trga in uporabnikov ter graditi na izkušnjah z zmogljivostmi in procesi certificiranja v EU (na primer okvir SOG-IS), hkrati pa bi moralo zagotoviti okvir, ki bi se lahko hitro prilagodil stanju prihodnjega razvoja digitalnih tehnologij;

- POUDARJA, da bi bilo treba pri krepitvi certificiranja na področju kibernetske varnosti v EU zajeti celoten spekter varnostnih zahtev, vse tja do najvišjih, kjer je treba dokazati odpornost proti zmogljivostim napadalcev. Ključni dejavniki uspeha bi bili zagotavljanje zanesljivega, preglednega in neodvisnega procesa za varnostno certificiranje s ciljem promoviranja razpoložljivosti zaupanje vlivajočih in varnih naprav, programske opreme in storitev v okviru enotnega trga in zunaj njega, priznavanje strokovnega znanja evropske industrije, vlad in strokovnjakov za ocenjevanje prek evropskih in svetovnih standardov[14] ter spoštovanje vloge držav članic v certifikacijskem postopku, predvsem kar zadeva ocenjevanje na višjih ravneh varnosti ter zlasti v povezavi z oceno osnovnih varnostnih potreb, znanj in spretnosti. Takšen certifikacijski okvir bi moral jamčiti tudi, da bo vsaka shema certificiranja na ravni EU sorazmerna s stopnjo zagotovila, ki je potrebna za uporabo proizvodov, storitev in/ali sistemov IKT, ter da bo omogočala čezmejno trgovanje, tako da bodo lahko podjetja vseh velikosti razvijala in prodajala nove proizvode tako na trgih EU kot drugod.

---

13 Prek globalnih standardov, razvitih v duhu kodeksa dobrih navad iz sporazuma WTO/TBT.

14 Prek evropskih in globalnih standardov, razvitih v duhu kodeksa dobrih navad iz sporazuma WTO/TBT.

21. POZDRAVLJA namero o ustanovitvi mreže strokovnih centrov za kibernetsko varnost, ki bi spodbujali razvoj in uvajanje tehnologije na področju kibernetske varnosti ter dajali dodaten zagon inovacijam v industriji EU na svetovni ravni pri razvoju tehnologij naslednje generacije in prelomnih tehnologij, kot so umetna inteligenca, kvantno računalništvo, veriga podatkovnih blokov (ang. *blockchain*) in varne digitalne identitete;

22. POUDARJA, da mora biti mreža strokovnih centrov za kibernetsko varnost vključujoča v razmerju do vseh držav članic ter njihovih obstoječih centrov odličnosti in pristojnosti, pri tem pa posebno pozornost namenjati dopolnjevanju, ter v tem kontekstu OPOZARJA NA načrtovani evropski raziskovalni center za kibernetsko varnost, katerega ključna vloga bi morala biti prav v osredotočenju na zagotavljanje dopolnjevanja in izogibanju podvajanja v okviru mreže strokovnih centrov za kibernetsko varnost in glede na druge agencije EU;

23. POUDARJA, da bi morala mreža strokovnih centrov za kibernetsko varnost obravnavati različna vprašanja, od raziskav do industrije, zaradi česar bi morala med drugim prispevati k doseganju cilja evropske strateške avtonomije;

24. v zvezi s predlagano mrežo strokovnih centrov za kibernetsko varnost PONOVNO POUDARJA, da mora EU prek svojih držav članic razviti evropsko zmogljivost za ocenjevanje trdnosti kriptografije, uporabljene v proizvodih in storitvah, ki so na voljo državljanom, podjetjem in vladam na enotnem digitalnem trgu, zavedajoč se, da so politike za kriptografijo ključni vidik nacionalne varnosti in so zato v pristojnosti držav članic;

25. POZIVA vse zadevne deležnike, naj povečajo naložbe v kibernetskovarnostne aplikacije novih tehnologij ter tako prispevajo k zagotavljanju kibernetske varnosti v vseh sektorjih evropskega gospodarstva;

26. POUDARJA pomen verodostojnega, zaupanje vlivajočega in usklajenega izvajanja storitev za kibernetsko varnost za institucije EU ter POZIVA KOMISIJO in druge institucije EU, naj v skladu s temi cilji nadalje razvijejo CERT-EU in v ta namen zagotovijo zadostna sredstva;

27. POZDRAVLJA poziv k priznanju pomembne vloge, ki jo imajo pri odkrivanju šibkih točk v obstoječih proizvodih in storitvah raziskovalci varnosti pri tretjih osebah, in POZIVA države članice, naj si izmenjujejo najboljše prakse v prid usklajenemu razkrivanju šibkih točk;

28. POUDARJA, da so za kibernetsko varnost odgovorni vsi, ter POZIVA EU in njene države članice, naj promovirajo digitalna znanja in spretnosti ter medijsko pismenost, ki bi uporabnikom pomagali zaščititi njihove digitalne informacije na spletu, hkrati pa jih ozaveščajo o tveganjih pri uporabi osebnih podatkov na internetu;

29. POZDRAVLJA poudarek, ki je v skupnem sporočilu namenjen izobraževanju, kibernetski higieni in ozaveščenosti v državah članicah in EU;

30. POZIVA KOMISIJO, naj hitro opravi oceno učinka, hkrati pa do sredine leta 2018 predlaga ustrezne pravne instrumente za izvedbo pobude za ustanovitev mreže strokovnih centrov za kibernetsko varnost ter evropskega raziskovalnega in strokovnega centra za kibernetsko varnost;

31. POZIVA države članice, naj:

- v informacijskih kampanjah dajejo prednost kibernetski ozaveščenosti, hkrati pa spodbujajo vključevanje kibernetske varnosti v akademske in izobraževalne programe ter programe poklicnega usposabljanja. Poseben poudarek bi bilo treba nameniti izobraževanju mladih in spodbujanju razvoja digitalnih spretnosti pri njih, da bi vzgojili strokovnjake, ki bodo pripravljeni na prihodnost ter na izzive na področju varnosti, gospodarstva in storitev;

- pospešijo prizadevanja za uvedbo specializiranih programov za kibernetsko varnost na visoki ravni, da strokovnjakov za kibernetsko varnost v EU ne bi več primanjkovalo, kot jih sedaj;

- pod okriljem agencije ENISA vzpostavijo učinkovito mrežo za sodelovanje kontaktnih točk za izobraževanje. Ta mreža bi si morala prizadevati za izboljšanje usklajevanja in izmenjave najboljših praks med državami članicami na področju izobraževanja in ozaveščanja o kibernetski varnosti, pa tudi za izboljšanje usposabljanja, vaj in krepitve zmogljivosti;

- razmislijo o razširitvi uporabe pravil iz direktive o varnosti omrežij in informacij tudi na javne uprave, ki sodelujejo v ključnih družbenih ali gospodarskih dejavnostih, če niso zajete že v nacionalni zakonodaji in če je to ustrezno, ter zagotovijo usposabljanje o kibernetski varnosti tudi v javnih upravah, glede na vlogo, ki jo imajo v naši družbi in gospodarstvu.

Poglavje II

RAZVOJ ZMOGLJIVOSTI EU ZA PREPREČEVANJE ZLONAMERNIH KIBERNETSKIH DEJAVNOSTI, ODVRAČANJE OD NJIH, NJIHOVO ODKRIVANJE IN ODZIVANJE NANJE

32. POUDARJA, da bi posebno hud kibernetski incident ali kriza lahko bila zadosten razlog, da država članica uveljavi solidarnostno klavzulo[15] in/ali klavzulo o vzajemni pomoči[16];

33. POZDRAVLJA sprejetje „Okvira za skupni diplomatski odziv EU na zlonamerne kibernetske dejavnosti“, ki je prispevek k preprečevanju konfliktov, sodelovanju in stabilnosti v kibernetskem prostoru, saj so v njem oprdeljeni ukrepi v okviru SZVP, vključno z omejevalnimi ukrepi, ki jih je mogoče uporabiti za preprečevanje zlonamernih kibernetskih dejavnosti in odzivanje nanje, ter POZIVA ESZD in države članice, naj imajo iz tega okvira redne vaje;

---

15 Člen 222 PDEU.
16 Člen 42(7) PEU.

34. IZPOSTAVLJA potrebo po učinkovitem odzivanju na ravni EU na kibernetske incidente in krize velikih razsežnosti, ob spoštovanju pristojnosti držav članic, in potrebo po vključitvi kibernetski varnosti v obstoječe mehanizme kriznega upravljanja na ravni EU[17]. Da bi to dosegli, SE ZAVZEMA za redne vaje na ravni EU iz odzivanja na kibernetske incidente velikih razsežnosti – od diplomatsko-strateškega do tehničnega –, kar naj bo oprto na ustrezne okvire in postopke[18], ki se po potrebi še izpilijo;

35. IZPOSTAVLJA pomen dobro integriranega odzivanja in mehanizmov izmenjave informacij med različnimi akterji, ki so odločilni za zagotavljanje kibernetske varnosti v Evropi, tudi med pristojnimi organi EU in organi držav članic. Takšne mehanizme bo treba preskusiti in preveriti v sklopu vaj iz kibernetske varnosti na ravni EU ter jih po potrebi formalizirati z ustreznimi sporazumi;

36. OPOZARJA NA možnost, da se – če Komisija predloži predlog za ustanovitev sklada za nujno odzivanje na krize na področju kibernetske varnosti ob že potekajočih prizadevanjih držav članic in v mejah razpoložljivih sredstev (zlasti v večletnem finančnem okviru EU) – preuči pomoč državam članicam pri odzivanju na kibernetske incidente velikih razsežnosti in njihovem obvladovanju, pod pogojem, da ima država članica že pred incidentom vzpostavljen previdnostni sistem kibernetske varnosti, vključno z dosledno implementacijo direktive o varnosti omrežij in informacij, ter preskušena okvira za obvladovanje tveganja in nadzor na nacionalni ravni;

37. PRIZNAVA vse večjo povezanost kibernetske varnosti in obrambe ter POZIVA k pospešitvi sodelovanja na področju kibernetske obrambe, tudi s spodbujanjem sodelovanja med civilnimi in vojaškimi akterji, ki se odzivajo na incidente, ter k nadaljevanju krepitve kibernetske varnosti misij in operacij v okviru SVOP;

---

17 Dok. C/2017/6100 final.
18 Dok. 9916/17 in C/2017/6100 final.

38. POUDARJA, da bi bilo po možnosti treba v celoti izrabiti prednosti predlaganih obrambnih pobud za pospešitev razvoja ustreznih kibernetskih zmogljivosti v Evropi, ter PRIZNAVA ne le obetavnost morebitne priprave projektov na področju kibernetske obrambe v okviru PESCO, če bi države članice, udeležene pri PESCO, to štele za potrebno, temveč PRIZNAVA tudi vlogo, ki jo imata tehnološka in industrijska baza evropske obrambe in širša civilna kibernetskovarnostna industrijska baza pri zagotavljanju sredstev državam članicam za vzdrževanje njihove kibernetske varnosti in obrambnih interesov;

39. JE SEZNANJEN s predlogom Komisije, naj se do konca leta 2018 vzpostavi platforma za usposabljanje in izobraževanje s področja kibernetske obrambe, in POUDARJA, da bi platforma morala pomeniti oplemenitenje možnosti za usposabljanje in izobraževanje v državah članicah ter bi pri njej moralo biti zagotovljeno dopolnjevanje z drugimi prizadevanji in pobudami EU, zlasti EAVO in EDA;

40. POZIVA EU in njene države članice, naj bodo odzivne, ko gre za nevarnost z IKT podprte kraje intelektualne lastnine, vključno s poslovnimi skrivnostmi ali drugimi zaupnimi poslovnimi informacijami, storjene z namenom, da se podjetjem ali gospodarskim sektorjem zagotovijo konkurenčne prednosti;

41. PRIZNAVA, da se je treba lotiti reševanja problema kaznivih dejanj v kibernetskem prostoru, tudi tistih v temnem spletu (ang. *Darkweb*), spolnega izkoriščanja otrok na spletu, pa tudi prevar in ponarejanja negotovinskih plačilnih sredstev, zlasti s prizadevanji za boljšo obveščevalno podobo, izvajanjem skupnih preiskav in izmenjevanjem operativne podpore;

42. POZDRAVLJA delo EU in njenih držav članic pri spoprijemanju z izzivi, ki jih predstavljajo sistemi, ki zločincem in teroristom dopuščajo pristojnim organom nedostopno komuniciranje, ter POUDARJA, da se je pri tem delu treba zavedati, da je močno in zaupanje uživajoče šifriranje zelo pomembno za kibernetsko varnost in zaupanje v enotni digitalni trg ter zagotavljanje spoštovanja človekovih pravic in temeljnih svoboščin;

43. POSEBEJ POUDARJA pomen zalaganja organov kazenskega pregona z orodji, ki omogočajo odkrivanje, preiskovanje in pregon kibernetskega kriminala, tako da kazniva dejanja v kibernetskem prostoru ne bi ostala neopažena ali nekaznovana, in POZDRAVLJA prispevek Evropske pravosodne mreže za kibernetsko kriminaliteto v boju proti kriminalu s sodelovanjem med pravosodnimi organi;

44. POUDARJA pomen zagotavljanja usklajenega stališča EU za učinkovito oblikovanje evropskih in globalnih odločitev glede upravljanja interneta v krogu številnih deležnikov, na primer ko gre za zagotavljanje hitro dostopnih in točnih podatkovnih zbirk naslovov IP in imen domen WHOIS, tako da bodo zmogljivosti kazenskega pregona in javni interesi varni;

45. POUDARJA, kako pomembno je, da se preide na internetni protokol IPv6, ki je nepogrešljiv za razvoj interneta stvari v ustreznem obsegu ter za izboljšanje ugotavljanja storilcev pri kriminalu v kibernetskem prostoru;

46. IZRAŽA PODPORO prizadevanjem, ki potekajo v zvezi s čezmejnim dostopom do elektronskih dokazov, reševanjem vprašanja hrambe podatkov in izzivi, ki jih za kazenski postopek predstavljajo sistemi, ki zločincem in teroristom dopuščajo pristojnim organom nedostopno komuniciranje, zavedajoč se, da je treba spoštovati človekove pravice in temeljne svoboščine ter varstvo podatkov;

47. POZIVA Komisijo, naj:

- do decembra 2017 predloži poročilo o napredku pri izvajanju praktičnih ukrepov za izboljšanje čezmejnega dostopa do elektronskih dokazov;
- v začetku leta 2018 predloži zakonodajni predlog za izboljšanje čezmejnega dostopa do elektronskih dokazov;

48. POZIVA Europol, agencijo ENISA in Eurojust, naj:

- še naprej krepijo sodelovanje v boju proti kibernetski kriminaliteti, tako med seboj kot z drugimi relevantnimi deležniki, vključno z mrežo CSIRT, Interpolom, zasebnim sektorjem in akademskimi krogi, ter s tem dosegajo sinergije in dopolnjevanja, v skladu z mandatom in pristojnostjo vsakega od njih;

- skupaj z državami članicami prispevajo k usklajenemu pristopu za odzivanje kazenskega pregona EU na kibernetske incidente in krize velikih razsežnosti v dopolnilo postopkom, začrtanim v ustreznih okvirih[19];

49. POZIVA EU in njene države članice, naj se še naprej trudijo:

- za premostitev ovir za preiskovanje kriminala in učinkovito kazensko pravosodje v kibernetskem prostoru, pa tudi za izboljšanje mednarodnega sodelovanja in usklajevanja v boju proti kriminalu v kibernetskem prostoru;

- za premagovanje izzivov, ki jih predstavljajo tehnologije, namenjene anonimizaciji, zavedajoč se, da je močno in zaupanje uživajoče šifriranje zelo pomembno za kibernetsko varnost in zaupanje v enotni digitalni trg;

- za oblikovanje odločitev o upravljanja interneta, ki imajo posledice za zmogljivosti kazenskega pregona za boj proti kriminalu v kibernetskem prostoru;

[19] Dok. 9916/17 in C/2017/6100 final.

Poglavje III

KREPITEV MEDNARODNEGA SODELOVANJA ZA ODPRT, SVOBODEN, MIROLJUBEN IN VAREN KIBERNETSKI PROSTOR

50. PRIZNAVA, da je zagotavljanje kibernetske varnosti globalen izziv, ki terja učinkovito globalno sodelovanje vseh akterjev, pa tudi, da je treba poseben poudarek nameniti spoštovanju demokratičnih vrednot in načel odprtega, svobodnega, miroljubnega in varnega globalnega kibernetskega prostora, ter ob upoštevanju tega

51. EU in njene države članice POZIVA, naj se zavzamejo za oblikovanje strateškega okvira za preprečevanje konfliktov, sodelovanje in stabilnost v kibernetskem prostoru, ki bo temeljil na uporabi obstoječega mednarodnega prava, še prav posebej pa na Ustanovni listini OZN v celoti, razvoju in uporabi univerzalnih norm odgovornega ravnanja držav in na regionalnih ukrepih za krepitev zaupanja med državami;

52. PRIZNAVA vlogo Organizacije združenih narodov pri nadaljnjem razvoju norm odgovornega ravnanja držav v kibernetskem prostoru in OPOZARJA, da se je z zaključki razprav v ustrezni skupini vladnih strokovnjakov pod okriljem Organizacije združenih narodov z leti oblikoval soglasen niz norm in priporočil[20], ki jih je Generalna skupščina vztrajno potrjevala in bi jih države morale uporabiti kot podlago za odgovorno ravnanje držav v kibernetskem prostoru;

53. PRIZNAVA, da te norme odgovornega ravnanja držav slednjim načeloma preprečujejo zavestno dopuščati uporabo njihovega ozemlja za kršitve mednarodnega prava, od njih zahtevajo odzivanje na ustrezna zaprosila za pomoč s strani druge države, katere kritična infrastruktura je tarča zlonamernih dejanj, podprtih z IKT, ki izvirajo z njihovega ozemlja, pa tudi sprejemanje ustreznih ukrepov za zaščito kritične infrastrukture pred grožnjami, podprtimi z IKT.

54. PRIZNAVA, da se EU, Nato in njune države članice soočajo z grožnjami in nevarnostmi, ki so jim skupne, PONAVLJA, kako pomembno je, da se sodelovanje med EU in Natom na področju kibernetske varnosti in obrambe nadaljuje ob doslednem spoštovanju načel vključenosti, vzajemnosti in avtonomnosti odločanja EU ter v skladu s sklepi z dne 6. decembra 2016 o izvajanju skupne izjave predsednika Evropskega sveta, predsednika Evropske komisije in generalnega sekretarja Organizacije Severnoatlantske pogodbe[20];

55. POZIVA EU in njene države članice, naj podpirajo in spodbujajo pripravo regionalnih ukrepov za krepitev zaupanja, ki so nepogrešljiv element, ko gre za poglabljanje sodelovanja, izboljšanje preglednosti in zmanjševanje tveganja za konflikte. Z izvajanjem ukrepov za krepitev zaupanja na področju kibernetske varnosti v okviru OVSE in drugih regionalnih forumov se bo predvidljivost ravnanja držav povečala, kibernetski prostor pa še dodatno stabiliziral;

56. PONOVNO POTRJUJE, da bo EU še naprej gojila svoje temeljne vrednote, ko gre za varstvo človekovih pravic in temeljnih svoboščin, pri čemer se bo opirala na Smernice EU o človekovih pravicah na spletu. EU prav tako poudarja, kako pomembno je, da so v upravljanje interneta vključeni vsi deležniki, tudi akademski krogi, civilna družba in zasebni sektor;

57. POZIVA EU in njene države članice, naj spodbujajo krepitev kibernetskih zmogljivosti v tretjih državah, pri čemer naj se posebna prednost nameni državam v sosedstvu EU in državam v razvoju, v katerih se povezljivost naglo povečuje, pri spopadanju s kibernetsko kriminaliteto in pri razvoju kibernetske odpornosti, v skladu s temeljnimi vrednotami EU. Za uveljavljanje prizadevanj EU na tem področju bi bilo treba vzpostaviti mrežo EU za razvoj zmogljivosti na področju kibernetske varnosti in pripraviti smernice EU za razvoj zmogljivosti na področju kibernetske varnosti, kar bi se moralo dopolnjevati z obstoječimi mehanizmi in strukturami;

---

[20] Dok. 15283/16.

58. POUDARJA napredek, dosežen pri sodelovanju med EU in Natom na področju kibernetske obrambe in varnosti ter pri njegovemu razvoju, kar zadeva usposabljanje, izobraževanje in koncepte, brez nepotrebnega podvajanja dela, kjer se zahteve prekrivajo, pa tudi glede spodbujanja interoperabilnosti prek zahtev in standardov za kibernetsko obrambo, ter POZIVA k nadaljevanju sodelovanja pri vajah iz kibernetske obrambe (štabna raven) in izmenjavi dobrih praks v zvezi s kriznim upravljanjem, brez nepotrebnega podvajanja dela, kjer se zahteve prekrivajo, ob doslednem spoštovanju politike EU glede vaj ter načel vključenosti, vzajemnosti in avtonomije odločanja EU;

59. PRIZNAVA, da Konvencija Sveta Evrope o kibernetski kriminaliteti (Budimpeška konvencija) predstavlja učinkovit pravni standard kot vodilo nacionalni zakonodaji o kibernetski kriminaliteti, ter POZIVA vse države, naj oblikujejo primerne nacionalne pravne okvire in sodelujejo v tem, že obstoječem mednarodnem okviru, ki ga nudi Budimpeška konvencija;

60. ŽELI SPOMNITI na dosežke pri dvostranskih dialogih EU o kibernetskih vprašanjih in poziva k nadaljnjemu trudu za olajšanje sodelovanja na področju kibernetske varnosti s tretjimi državami;

61. ŽELI SPOMNITI, da ima EU robusten in pravno zavezujoč mehanizem nadzora nad izvozom, ki temelji na odločitvah in najboljših praksah, razvitih v okviru mednarodnih neproliferacijskih ureditev, JE SEZNANJEN z razpravami, ki potekajo v Svetu, da bi se našle najboljše rešitve za dodatno izboljšanje delovanja teh nadzornih mehanizmov, in POZIVA države članice, naj v okviru ustreznih mednarodnih ureditev za nadzor nad izvozom (npr. Wassenaarske ureditve), še naprej načenjajo vprašanje odločilnih aplikacij novih tehnologij za kibernetsko varnost, da se zagotovi učinkovit nadzor nad odločilnimi kibernetskovarnostnimi tehnologijami jutrišnjega dne.

62. Ti sklepi se bodo udejanjali prek akcijskega načrta, ki ga bo Svet sprejel pred koncem leta 2017, v smislu nadaljnjega ukrepanja na podlagi sklepov Evropskega sveta z dne 19. oktobra 2017[21]. Akcijski načrt je živ dokument in ga kot takega Svet redno pregleduje in posodablja.

---

[21] Dok. EUCO 14/17.