asioiden pääosasto) ja EU:n virastojen (muun muassa Europol, Frontex, Tautien ehkäisyn ja valvonnan eurooppalainen keskus), tuottamat tiedot;

o

o o

48. kehottaa puhemiestä välittämään tämän päätöslauselman komission varapuheenjohtajalle / korkealle edustajalle, neuvostolle ja komissiolle, jäsenvaltioiden parlamenteille, Naton parlamentaariselle yleiskokoukselle sekä Naton pääsihteerille.

P7_TA(2012)0457

Tietoverkkoturvallisuus ja -puolustus

Euroopan parlamentin päätöslauselma 22. marraskuuta 2012 tietoverkkoturvallisuudesta ja -puolustuksesta (2012/2096(INI))

(2015/C 419/22)

Euroopan parlamentti, joka

— ottaa huomioon Eurooppa-neuvoston 11. ja 12. joulukuuta 2008 hyväksymän selvityksen Euroopan unionin turvallisuusstrategian täytäntöönpanosta,

— ottaa huomioon 23. marraskuuta 2001 tehdyn tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen,

— ottaa huomioon elintärkeiden tietoinfrastruktuureiden suojaamisesta 27. toukokuuta 2011 annetut neuvoston päätelmät sekä aikaisemmat tietoverkkoturvallisuutta koskevat neuvoston päätelmät,

— ottaa huomioon 19. toukokuuta 2010 annetun komission tiedonannon Euroopan digitaalistrategiasta (COM(2010) 0245),

— ottaa huomioon 8. joulukuuta 2008 annetun neuvoston direktiivin 2008/114/EY Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista ([1]),

— ottaa huomioon komission äskettäisen tiedonannon (COM(2012)0140), jossa käsitellään Euroopan verkkorikostorjuntakeskuksen perustamista, joka on yksi sisäisen turvallisuuden strategian painopisteistä,

— ottaa huomioon Euroopan turvallisuusstrategian täytäntöönpanosta osana yhteistä turvallisuus- ja puolustuspolitiikkaa 10. maaliskuuta 2010 antamansa päätöslauselman ([2]),

— ottaa huomioon yhteisen turvallisuus- ja puolustuspolitiikan kehityksestä Lissabonin sopimuksen voimaantulon jälkeen 11. toukokuuta 2011 antamansa päätöslauselman ([3]),

— ottaa huomioon 22. toukokuuta 2012 antamansa päätöslauselman Euroopan unionin sisäisen turvallisuuden strategiasta ([4]),

— ottaa huomioon 27. syyskuuta 2011 antamansa päätöslauselman ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi kaksikäyttötuotteiden ja -teknologian vientiä koskevan yhteisön valvontajärjestelmän perustamisesta annetun asetuksen (EY) N:o 1334/2000 muuttamisesta ([5]),

— ottaa huomioon 12. kesäkuuta 2012 antamansa päätöslauselman ”Elintärkeiden tietoinfrastruktuureiden suojaaminen – saavutukset ja seuraavat vaiheet: kohti maailmanlaajuista verkkoturvallisuutta” ([6]),

---

([1]) EUVL L 345, 23.12.2008, s. 75.
([2]) EUVL C 349 E, 22.12.2010, s. 63.
([3]) Hyväksytyt tekstit, P7_TA(2011)0228.
([4]) Hyväksytyt tekstit, P7_TA(2012)0207.
([5]) Hyväksytyt tekstit, P7_TA(2011)0406.
([6]) Hyväksytyt tekstit, P7_TA(2012)0237.

Torstai 22. marraskuuta 2012

— ottaa huomioon YK:n ihmisoikeusneuvoston 5. heinäkuuta 2012 antaman päätöslauselman ”The promotion, protection and enjoyment of human rights on the Internet” ([1]), jossa tunnustetaan ihmisoikeuksien suojelun merkitys ja verkossa tapahtuvan tiedonkulun vapauden merkitys,

— ottaa huomioon Chicagossa 20. toukokuuta 2012 pidetyn huippukokouksen päätelmät,

— ottaa huomioon Euroopan unionista tehdyn sopimuksen V osaston,

— ottaa huomioon työjärjestyksen 48 artiklan;

— ottaa huomioon ulkoasiainvaliokunnan mietinnön (A7-0335/2012);

A. katsoo, että nykypäivän globalisoituneessa maailmassa EU:sta ja sen jäsenvaltioista on tullut erittäin riippuvaisia tietoverkon turvallisuudesta ja tietotekniikan ja digitaalitekniikan turvallisesta käytöstä sekä kestävistä ja luotettavista tietopalveluista ja niihin liittyvistä infrastruktuureista;

B. ottaa huomioon, että tieto- ja viestintätekniikoita käytetään myös painostusvälineinä; toteaa, että konteksti, jossa niitä käytetään, määrittää paljolti vaikutuksen, joka niillä voi olla myönteisenä voimana tai vastaavasti painostuksessa;

C. ottaa huomioon, että tietoverkkoon liittyvät haasteet, uhat ja hyökkäykset kasvavat dramaattista vauhtia ja ovat huomattava uhka kansallisvaltioiden sekä yksityisen sektorin turvallisuudelle, puolustukselle, vakaudelle ja kilpailukyvylle; toteaa, että tästä syystä tällaisia uhkia ei saisi pitää tulevaisuuden haasteina; toteaa, että suurin osa erittäin näkyvistä ja vahingollisista verkkoturvallisuuspoikkeamista on nyt luonteeltaan poliittisia; toteaa, että suurin osa verkkoturvallisuuspoikkeamista on edelleen alkeellisia mutta elintärkeään omaisuuteen kohdistuvista uhista on tulossa yhä kehittyneempiä ja ne antavat aihetta huolelliseen suojeluun;

D. ottaa huomioon, että tietoverkolla on maailmanlaajuisesti lähes kaksi miljardia keskenään kytköksissä olevaa käyttäjää ja että tietoverkosta on tullut vaikutusvaltaisin ja tehokkain tapa edistää demokraattisia ajatuksia ja saada ihmiset järjestäytymään näiden pyrkiessä toteuttamaan vapauspyrkimyksiään ja taistelemaan diktatuureja vastaan; toteaa, että epädemokraattisten ja autoritaaristen hallintojen käytössä tietoverkko muodostaa entistä voimakkaammin uhan yksilöiden oikeudelle ilmaisun- ja yhdistymisvapauteen; katsoo, että tästä syystä on hyvin tärkeää varmistaa, että tietoverkko pysyy avoimena ajatusten vapaalle vaihdolle, tiedonkululle ja itseilmaisulle;

E. ottaa huomioon, että EU:ssa ja jäsenvaltioissa kattavan ja yhtenäisen tietoverkkojen puolustusta ja turvallisuutta koskevan lähestymistavan kehittämisen tiellä on lukuisia esteitä, jotka ovat luonteeltaan poliittisia, lainsäädännöllisiä ja organisatorisia; ottaa huomioon, että tietoverkkoturvallisuuden ala on arkaluonteinen ja haavoittuva ja alan yhteisestä määritelmästä, yhteisistä normeista ja yhteisistä toimenpiteistä on pulaa;

F. toteaa, että EU:n toimielinten keskinäinen ja jäsenvaltioiden keskinäinen sekä toisaalta toimielinten ja jäsenvaltioiden välinen ja myös ulkopuolisten kumppaneiden kanssa harjoitettava tietojen vaihto ja koordinointi on edelleen riittämätöntä;

G. toteaa, että ”tietoverkkoturvallisuudesta” ja ”tietoverkkopuolustuksesta” ei ole selkeitä ja yhdenmukaistettuja EU:n ja kansainvälisen tason määritelmiä; toteaa, että se, mitä ymmärretään tietoverkkoturvallisuudella ja muulla keskeisellä terminologialla, vaihtelee huomattavasti eri maiden välillä;

H. ottaa huomioon, ettei EU ole vielä laatinut omia johdonmukaisia toimintalinjojaan elintärkeiden tietoinfrastruktuureiden suojaamisesta, joka edellyttäisi monialaista lähestymistapaa ja lisäisi turvallisuutta ja edistäisi perusoikeuksia;

I. ottaa huomioon, että EU on ehdottanut useita aloitteita siviilitason tietoverkkorikollisuuden torjumiseksi, uuden eurooppalaisen verkkorikostorjuntakeskuksen perustaminen mukaan luettuna, mutta siltä puuttuu konkreettinen turvallisuus- ja puolustussuunnitelma;

J. katsoo, että yksityisen sektorin, lainvalvontaviranomaisten, puolustuslaitosten ja muiden toimivaltaisten viranomaisten keskinäisen luottamuksen rakentaminen on erittäin tärkeää tietoverkkorikollisuuden torjumisen kannalta;

([1]) http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx

K. katsoo, että valtiollisten ja valtioista riippumattomien toimijoiden molemminpuolinen luottamus on myös luotettavan tietoverkkoturvallisuuden edellytys;

L. ottaa huomioon, että suurin osa sekä julkisen että yksityisen sektorin verkkoturvallisuuspoikkeamista jää ilmoittamatta tiedon arkaluonteisuuden vuoksi sekä siitä syystä, että ne saattaisivat vahingoittaa asianomaisten yritysten julkisuuskuvaa;

M. toteaa, että monet verkkoturvallisuuspoikkeamat johtuvat yksityisen ja julkisen verkkoinfrastruktuurin häiriönsietokyvyn ja toimintavarmuuden puutteesta, tietokantojen huonosta suojaamisesta tai turvaamisesta ja muista puutteista kriittisessä tietoinfrastruktuurissa; toteaa, että vain harvat jäsenvaltiot pitävät verkkonsa ja tietojärjestelmiensä sekä niihin liittyvien tietojen suojelua osana huolellisuusvelvollisuuttaan, mikä selittää sen, että huipputason turvatekniikkaan investoiminen sekä koulutukseen ja asianmukaisten ohjeiden laatimiseen panostaminen on riittämätöntä, ja ottaa huomioon, että erittäin monet jäsenvaltiot ovat riippuvaisia kolmansien maiden turvallisuustekniikasta, ja katsoo, että toimia on lisättävä tämän riippuvuuden vähentämiseksi;

N. toteaa, että suurin osa kansallista tai kansainvälistä turvallisuutta ja puolustusta uhkaavien korkean tason tietoverkkohyökkäysten tekijöistä jää tunnistamatta ja asettamatta syytteeseen; toteaa, ettei ole olemassa kansainvälisesti sovittua reagointitapaa sellaisiin tietoverkkohyökkäyksiin, joiden takana on valtio, eikä yhteisymmärrystä siitä, voitaisiinko tällaisen hyökkäyksen katsoa antavan oikeutuksen sotatoimiin;

O. ottaa huomioon, että Euroopan verkko- ja tietoturvaviraston (ENISA) tehtävänä on toimia välittäjänä jäsenvaltioiden suuntaan ja tukea tietoverkkoturvallisuuden alan hyvien käytänteiden vaihtoa antamalla suosituksia siitä, miten tietoverkkoturvallisuusstrategiaa voidaan kehittää, soveltaa ja ylläpitää, ja toteaa, että sillä on tukijan rooli kansallisissa verkkoturvallisuusstrategioissa, kansallisissa varautumissuunnitelmissa, elintärkeiden tietoinfrastruktuureiden (CIIP) suojaamista koskevien yleiseurooppalaisten ja kansainvälisten harjoitusten järjestämisessä ja kansallisia harjoituksia koskevien skenaarioiden laatimisessa;

P. ottaa huomioon, että EU:n jäsenvaltioista ainoastaan kymmenen oli virallisesti hyväksynyt kansallisen verkkoturvallisuusstrategian kesäkuuhun 2012 mennessä;

Q. ottaa huomioon, että tietoverkkopuolustus on yksi Euroopan puolustusviraston (EDA) keskeisistä painopistealueista, ja toteaa, että EDA on perustanut voimavarojen kehittämissuunnitelman mukaisen tietoverkkoturvallisuutta käsittelevän hankeryhmän ja että suurin osa jäsenvaltioista on ryhtynyt toimiin kerryttääkseen kokemuksia ja esittääkseen suosituksia;

R. toteaa, että investoinnit tietoverkkoturvallisuutta ja -puolustusta koskevaan tutkimukseen ja kehittämiseen ovat erittäin tärkeitä turvallisuuden ja puolustuksen korkean tason edistämiseksi ja säilyttämiseksi; toteaa, että puolustusta koskevat tutkimus- ja kehittämismenot ovat vähentyneet sen sijaan, että niiden osuutta olisi korotettu sovittuun kahteen prosenttiin puolustuksen kokonaismenoista;

S. ottaa huomioon, että kansalaisten tietoverkkoturvallisuutta koskevan tietämyksen ja valistamisen lisäämisen olisi oltava jokaisen kattavan tietoverkkoturvallisuusstrategian perustana;

T. ottaa huomioon, että turvallisuustoimenpiteiden ja sellaisten kansalaisoikeuksien välille kuin oikeus yksityisyyteen, tietosuojaan ja ilmaisunvapauteen, on saatava aikaan selkeä tasapaino SEUT-sopimuksen mukaisesti uhraamatta toista toisen kustannuksella;

U. ottaa huomioon, että yksilöiden oikeutta yksityisyyteen on kunnioitettava ja suojeltava entistä paremmin, kuten EU:n perusoikeuskirjassa ja SEUT-sopimuksen 16 artiklassa määrätään; katsoo, ettei laitosten ja puolustuselinten tarvetta turvata ja puolustaa tietoverkkoa kansallisella tasolla saisi koskaan käyttää oikeuttamaan oikeuksien ja vapauksien rajoittamista millään tavalla tietoverkossa tai tiedonvälityksessä;

V. katsoo, että internetin maailmanlaajuinen ja rajaton luonne edellyttää uusia kansainvälisen yhteistyön ja hallinnan muotoja, jossa on monia osallistujia;

W. ottaa huomioon, että hallitukset ovat yhä suuremmassa määrin riippuvaisia yksityisistä toimijoista elintärkeän infrastruktuurinsa turvaamisessa;

X. ottaa huomioon, ettei Euroopan ulkosuhdehallinto (EUH) ole vielä ennakoivasti sisällyttänyt tietoverkkoturvallisuusnäkökulmaa suhteisiinsa kolmansien maiden kanssa;

Y. ottaa huomioon, että vakausväline on toistaiseksi ainoa EU:n ohjelma, joka on suunniteltu siihen tarkoitukseen, että sillä voidaan puuttua äkillisiin kriiseihin tai kansalliset ja alueelliset rajat ylittäviin turvallisuusongelmiin, myös tietoverkkoturvallisuuteen liittyviin uhkiin;

Z. ottaa huomioon, että yhteinen reagoiminen tietoverkkouhkiin EU:n ja Yhdysvaltojen verkkoturvallisuus- ja verkkorikollisuustyöryhmän välityksellä on yksi tärkeimmistä EU:n ja Yhdysvaltojen suhteiden painopistealueista;

EU:n toimet ja koordinointi

1. panee merkille, että tietoverkkoon liittyvät uhat ja hyökkäykset valtion ja hallinnon elimiä sekä sotilaallisia ja kansainvälisiä elimiä vastaan ovat kasvava uhka ja niitä esiintyy yhä useammin sekä EU:ssa että maailmanlaajuisesti ja toteaa, että on merkittäviä syitä olla huolestunut siitä, että valtiolliset ja muut toimijat, erityisesti terroristi- ja rikollisjärjestöt, kykenevät kohdistamaan hyökkäyksen EU:n toimielinten ja sen jäsenvaltioiden elintärkeisiin tieto- ja viestintäjärjestelmiin ja infrastruktuureihin ja mahdollisesti aiheuttamaan merkittävää vahinkoa, kineettiset vaikutukset mukaan lukien;

2. korostaa sen vuoksi, että näihin haasteisiin vastaamiseksi tarvitaan EU:n tason yleinen koordinoitu linjaus sellaisen kattavan EU:n tietoverkkoturvallisuusstrategian muodossa, jossa esitetään tietoverkkoturvallisuutta ja -puolustusta ja puolustukseen liittyvää tietoverkkohyökkäystä koskeva yhteinen määritelmä ja yhteinen toimintavisio ja jossa olisi otettava huomioon nykyisten virastojen ja elinten lisäarvo sekä sellaisilta jäsenvaltioilta omaksuttavat hyvät käytänteet, joilla on jo kansalliset tietoverkkoturvallisuusstrategiat; tähdentää koordinoinnin ja synergioiden luomisen merkitystä unionissa, sillä niiden avulla voidaan tukea eri sotilaallisten ja siviilialoitteiden, -ohjelmien sekä -toimien yhdistämistä; korostaa, että tällaisella strategialla olisi taattava joustavuus ja sitä olisi päivitettävä säännöllisesti, jotta sitä voitaisiin mukauttaa tietoverkon nopeasti muuttuvan luonteen edellyttämällä tavalla;

3. kehottaa komissiota ja unionin ulkoasioiden ja turvallisuuspolitiikan korkeaa edustajaa pohtimaan jäsenvaltioon kohdistuvan vakavan tietoverkkohyökkäyksen mahdollisuutta tulevassa ehdotuksessaan yhteisvastuulausekkeen täytäntöönpanoa koskevista järjestelyistä (SEUT-sopimuksen 222 artikla); katsoo lisäksi, että vaikka kansallisen turvallisuuden vaarantavat tietoverkkohyökkäykset on vielä määriteltävä yhteisin termein, niihin voitaisiin soveltaa keskinäistä puolustusta koskevaa lauseketta (SEU-sopimuksen 42 artiklan 7 kohta) rajoittamatta kuitenkaan suhteellisuusperiaatteen noudattamista;

4. korostaa, että YTPP:n on varmistettava, että EU:n sotilaallisiin operaatioihin ja siviilioperaatioihin osallistuvia joukkoja suojellaan tietoverkkohyökkäyksiltä; painottaa, että tietoverkkopuolustuksesta olisi tehtävä YTPP:n aktiivinen valmius;

5. korostaa, että kaikkien EU:n verkkoturvallisuutta koskevien toimintalinjojen olisi perustuttava digitaalisten vapauksien maksimaaliseen suojeluun ja säilyttämiseen sekä ihmisoikeuksien kunnioittamiseen verkossa, ja ne olisi suunniteltava tähän tarkoitukseen; katsoo, että internet ja tieto- ja viestintätekniikka olisi sisällytettävä EU:n ulko- ja turvallisuuspolitiikkaan tämän pyrkimyksen edistämiseksi;

6. kehottaa komissiota ja neuvostoa yksiselitteisesti tunnustamaan digitaaliset vapaudet perusoikeuksiksi ja välttämättömiksi edellytyksiksi yleismaailmallisten ihmisoikeuksien toteutumiselle; korostaa, että jäsenvaltioiden olisi pyrittävä siihen, etteivät ne koskaan vaaranna kansalaistensa oikeuksia ja vapauksia kehittäessään toimia verkkouhkien ja -hyökkäysten torjumiseksi ja että niillä olisi oltava asianmukaiset lainsäädännölliset erot siviili- ja sotilaallisen tason verkkoturvallisuuspoikkeamien välillä; kehottaa varovaisuuteen rajoitusten asettamisessa sille, miten kansalaiset voivat käyttää tieto- ja viestintätekniikan välineitä;

7. kehottaa neuvostoa ja komissiota laatimaan yhdessä jäsenvaltioiden kanssa verkkopuolustusta koskevan valkoisen kirjan, jossa annetaan selkeät määritelmät ja kriteerit siviili- ja sotilaallisten verkkohyökkäysten eri tasojen erottamiseksi niiden vaikutinten ja vaikutusten mukaan sekä reagoinnin eri tasojen erottamiseksi, mukaan lukien rikoksentekijöiden tutkinta, selvittäminen ja syytteeseenpano;

8. toteaa selkeän tarpeen ajantasaistaa Euroopan turvallisuusstrategia, jotta määritetään ja löydetään keinot yksittäisten, verkostoon kuuluvien ja valtion tukemien verkkohyökkääjien etsimiseksi ja syytteeseen panemiseksi;

EU:n taso

9. tähdentää EU:n toimielinten ja virastojen sisällä ja niiden kesken toteutettavan horisontaalisen yhteistyön ja koordinoinnin merkitystä tietoverkkoturvallisuudelle;

10. korostaa, että uudet teknologiat asettavat haasteen tavalle, jolla hallitukset hoitavat perinteisiä ydintehtäviä; vahvistaa, että puolustus- ja turvallisuuspolitiikka kuuluvat viime kädessä hallitusten toimivaltaan, asiaankuuluva demokraattinen valvonta mukaan lukien; panee merkille yksityisten toimijoiden yhä tärkeämmän roolin turvallisuus- ja puolustustehtävien hoitamisessa, usein ilman avoimuutta, vastuuvelvollisuutta tai demokraattisia valvontamekanismeja;

11. korostaa, että käyttäessään uusia tekniikoita turvallisuus- ja puolustuspolitiikan alalla hallitusten on noudatettava kansainvälisen julkisoikeuden ja humanitaarisen oikeuden perusperiaatteita; viittaa EU:n jäsenvaltioiden kuten Viron arvokkaaseen kokemukseen verkkoturvallisuutta sekä verkkopuolustusta koskevien toimintalinjojen määrittelyssä ja suunnittelussa;

12. toteaa, että on arvioitava EU:n tietojärjestelmiin ja infrastruktuuriin kohdistuvien tietoverkkohyökkäysten yleistä tasoa; korostaa tässä yhteydessä, että EU:n toimielinten valmiutta torjua mahdollisia tietoverkkohyökkäyksiä on arvioitava jatkuvasti; painottaa erityisesti tarvetta vahvistaa elintärkeitä tietoinfrastruktuureita;

13. korostaa myös, että tarvitaan tietoa tietojärjestelmien puutteista sekä niihin kohdistuvien uusien uhkien hälytyksistä ja varoituksista;

14. panee merkille, että äskettäiset eurooppalaisiin tietoverkkoihin sekä valtiollisiin tietojärjestelmiin kohdistuneet hyökkäykset ovat aiheuttaneet huomattavia taloudellisia ja turvallisuuteen liittyviä vahinkoja, joiden laajuutta ei ole vielä toistaiseksi riittävästi arvioitu;

15. kehottaa kaikkia EU:n toimielimiä kehittämään omia järjestelmiään koskevia tietoverkkoturvallisuusstrategioita ja varautumissuunnitelmia mahdollisimman pikaisesti;

16. kehottaa kaikkia EU:n toimielimiä sisällyttämään riskianalyyseihinsä sekä kriisinhallintasuunnitelmiinsa tietoverkkokriisien hallintaa koskevan ongelman; kehottaa myös kaikkia EU:n toimielimiä tarjoamaan tietoverkkoturvallisuutta koskevaa tietämystä lisäävää koulutusta koko henkilöstölleen; ehdottaa tietoverkkoharjoitusten järjestämistä kerran vuodessa pelastusharjoitusten tavoin;

17. korostaa tietoturvaloukkauksiin ja niiden ennaltaehkäisyyn keskittyvän ryhmän (EU-CERT) ja kansallisten tietotekniikan kriisiryhmien tehokkaan kehittämisen sekä kansallisten varautumissuunnitelmien laatimisen merkitystä siinä tapauksessa, että tositoimiin on ryhdyttävä; pitää myönteisenä, että kaikki EU:n jäsenvaltiot ovat perustaneet kansallisen tietotekniikan kriisiryhmän toukokuuhun 2012 mennessä; vaatii kehittämään edelleen kansallisia tietotekniikan kriisiryhmiä ja EU:n tietotekniikan kriisiryhmää, jota voidaan hyödyntää tarvittaessa vuorokauden ympäri; korostaa, että on tarkasteltava tämän alan yksityisen ja julkisen sektorin kumppanuuksien toteutettavuutta;

18. toteaa, että ensimmäinen yleiseurooppalainen suuren mittakaavan verkkoturvallisuusharjoitus ”Cyber Europe 2010”, joka toteutettiin monien jäsenvaltioiden voimin ja ENISAn johdolla, osoittautui hyödylliseksi toimenpiteeksi ja esimerkiksi hyvistä käytänteistä; painottaa myös tarvetta luoda elintärkeiden infrastruktuureiden varoitusjärjestelmä EU:n tasolla mahdollisimman pian;

19. korostaa yleiseurooppalaisten laajamittaisten verkkoturvallisuusharjoitusten sekä yhtenäisten uhka-arviota koskevien vaatimusten määrittämisen merkitystä;

20. kehottaa komissiota tutkimaan EU:n tietoverkkokoordinointia koskevan viran tarpeellisuutta ja toteutettavuutta;

21. ottaa huomioon, että sekä verkkojärjestelmien ja infrastruktuurien asianmukainen puolustaminen että niihin kohdistettava hyökkäys edellyttää suurta taitoa ja katsoo, että olisi harkittava mahdollisuutta laatia ”valkohattuhakkereiden” hyödyntämiseen perustuva strategia komission, neuvoston ja jäsenvaltioiden kesken; panee merkille, että ”aivovuodon” mahdollisuus on tällaisissa tapauksissa suuri ja että erityisesti alaikäisillä, jotka on tuomittu tällaisista hyökkäyksistä, on hyvät edellytykset sekä rehabilitointiin että yhteistyöhön puolustusvirastojen ja -elinten kanssa;

Euroopan puolustusvirasto (EDA)

22. suhtautuu myönteisesti hiljattain esitettyihin tietoverkkopuolustusta koskeviin aloitteisiin ja hankkeisiin ja erityisesti asiaa koskevien tietoverkkoturvallisuuteen ja -puolustukseen liittyvien tietojen sekä haasteiden ja tarpeiden kokoamiseen ja kartoittamiseen ja kehottaa jäsenvaltioita tekemään enemmän yhteistyötä myös sotilaallisella tasolla EDA:n kanssa verkkopuolustuksen alalla;

Torstai 22. marraskuuta 2012

23. korostaa olevan tärkeää, että jäsenvaltiot tekevät EDA:n kanssa tiivistä yhteistyötä tietoverkkopuolustukseen liittyvien kansallisten valmiuksien kehittämiseksi; katsoo, että synergioiden luominen sekä voimavarojen keskittäminen ja jakaminen Euroopan tasolla on erittäin tärkeää tehokkaan tietoverkkopuolustuksen kannalta sekä EU:n että kansallisella tasolla;

24. kehottaa EDA:a lisäämään yhteistyötään Naton, kansallisten ja kansainvälisten huippuyksiköiden, nopeampaa vastaamista verkkohyökkäyksiin edistävän Europolissa toimivan Euroopan verkkorikostorjuntakeskuksen ja erityisesti tietoverkkojen puolustamiseen erikoistuneen Cooperative Cyber Defence Centre of Excellence -osaamiskeskuksen (CCDCOE) kanssa ja keskittymään valmiuksien kehittämiseen ja koulutukseen sekä tietojen ja käytänteiden vaihtoon;

25. panee huolestuneena merkille, että ainoastaan yksi jäsenvaltio saavutti kahden prosentin tason puolustusalan tutkimus- ja kehittämistoimien menoissa vuoteen 2010 mennessä ja että viisi jäsenvaltiota ei käyttänyt lainkaan määrärahoja tutkimus- ja kehittämistoimiin; kehottaa EDA:a yhdessä jäsenvaltioiden kanssa keskittämään voimavaroja ja investoimaan tehokkaasti tutkimus- ja kehittämisyhteistyöhön ja kiinnittämään erityistä huomiota tietoverkkoturvallisuuteen ja -puolustukseen;

Jäsenvaltiot

26. kehottaa jäsenvaltioita kehittämään ja täydentämään kansallisia tietoverkkoturvallisuus- ja tietoverkkopuolustusstrategioitaan viipymättä ja turvaamaan vakaan päätöksenteko- ja sääntely-ympäristön, kattavat riskinhallintamenettelyt ja asianmukaiset valmistelutoimet ja -mekanismit; kehottaa ENISAa auttamaan jäsenvaltioita; tuo julki tukensa ENISAlle, joka on laatimassa hyvien käytänteiden opasta, jossa hyvien käytänteiden lisäksi esitetään suosituksia siitä, miten tietoverkkoturvallisuusstrategia on laadittava ja pantava täytäntöön ja miten sitä on ylläpidettävä;

27. kehottaa kaikkia jäsenvaltioita luomaan tietoverkkoturvallisuuteen ja -puolustukseen tarkoitettuja yksiköitä sotilaallisen rakenteensa yhteyteen tavoitteena yhteistyön harjoittaminen EU:n muiden jäsenvaltioiden vastaavien elinten kanssa;

28. kannustaa jäsenvaltioita ottamaan käyttöön aluetason erityistuomioistuimet, joiden tehtävänä on varmistaa, että tietojärjestelmiä vastaan tehdyistä hyökkäyksistä rangaistaan tehokkaammin; painottaa tarvetta edistää kansallisten lakien mukauttamista siten, että ne voidaan sovittaa tekniikoiden ja käyttötapojen kehitykseen;

29. kehottaa komissiota jatkamaan toimiaan sellaisen johdonmukaisen ja tehokkaan eurooppalaisen linjauksen luomiseksi, jonka avulla voidaan välttää tarpeettomat aloitteet, kannustaa ja tukea jäsenvaltioiden pyrkimyksiä kehittää yhteistyöjärjestelmiään ja tehostaa tietojen vaihtoa; katsoo, että olisi syytä vakiinnuttaa jäsenvaltioiden välisen yhteistyön ja tietojenvaihdon pakollinen vähimmäistaso;

30. kehottaa jäsenvaltioita laatimaan kansallisia valmiussuunnitelmia ja sisällyttämään tietoverkkokriisien hallinta kriisinhallintasuunnitelmiin ja riskianalyyseihin; korostaa lisäksi julkisten laitosten koko henkilöstölle annettavan tietoverkkoturvallisuuden perusteita koskevan riittävän koulutuksen merkitystä ja erityisesti oikeusalan elinten ja turvallisuuselinten jäsenille koulutusyksiköissä annettavan asianmukaisen koulutuksen merkitystä; kehottaa ENISAa ja muita asiaankuuluvia elimiä auttamaan jäsenvaltioita voimavarojen keskittämisessä ja vaihtamisessa sekä päällekkäisyyksien välttämisessä;

31. kehottaa jäsenvaltioita tekemään tutkimus- ja kehittämistyöstä yhden tietoverkkoturvallisuuden ja -puolustuksen keskeisistä ulottuvuuksista ja edistämään tietojärjestelmien suojeluun erikoistuneiden insinöörien koulutusta; kehottaa jäsenvaltioita toimimaan sitoumuksensa mukaisesti eli lisäämään tutkimukseen ja kehittämiseen liittyviä puolustusmenojaan vähintään kahteen prosenttiin siten, että erityistä huomiota kiinnitetään tietoverkkoturvallisuuteen ja -puolustukseen;

32. kehottaa komissiota ja jäsenvaltioita esittämään ohjelmia, joiden avulla voidaan edistää yleisesti niin yksityisten kuin yrityskäyttäjien tietoisuutta internetin ja tieto- ja viestintätekniikan turvallisesta käytöstä; ehdottaa, että komissio käynnistäisi tätä koskevan julkisen yleiseurooppalaisen koulutusaloitteen; kehottaa jäsenvaltioita sisällyttämään tietoverkkoturvallisuuden koulujen opetusohjelmiin mahdollisimman varhaisesta iästä;

Julkisen ja yksityisen sektorin yhteistyö

33. korostaa viranomaisten ja yksityisen sektorin välisen tarkoituksenmukaisen ja täydentävän sekä luottamuksen rakentamiseen tähtäävän tietoverkkoturvallisuusyhteistyön merkittävää roolia sekä EU:n että kansallisella tasolla; on tietoinen siitä, että asiaankuuluvien julkisten laitosten luotettavuuden ja tehokkuuden vahvistaminen entisestään vaikuttaa

osaltaan luottamuksen rakentamiseen sekä elintärkeän tiedon vaihtamiseen;

34. kehottaa yksityisen sektorin kumppaneita harkitsemaan sisäänrakennettuja turvallisuusratkaisuja uusien tuotteiden, laitteiden, palvelujen ja sovellusten suunnittelun yhteydessä; kehottaa soveltamaan avoimuutta koskevia vähimmäisvaatimuksia ja ottamaan käyttöön vastuumekanismeja yksityisen sektorin kanssa tehtävässä yhteistyössä, jotta voidaan ehkäistä ja torjua tietoverkkohyökkäyksiä;

35. korostaa, että elintärkeiden tietoinfrastruktuureiden suojaaminen sisältyy EU:n sisäisen turvallisuuden strategiaan, koska pyrkimyksenä on parantaa kansalaisten ja yritysten turvallisuutta verkkoympäristössä;

36. kehottaa käymään näiden osapuolten kanssa jatkuvaa vuoropuhelua tietojärjestelmien parhaasta käytöstä ja kestävyydestä sekä järjestelmiä koskevan vastuun jakamisesta, sillä se on edellytys näiden järjestelmien turvalliselle ja asianmukaiselle toiminnalle;

37. katsoo, että jäsenvaltioiden, EU:n ja yksityissektorin olisi ryhdyttävä yhteistyössä ENISAn kanssa toimiin, joilla voidaan parantaa tietojärjestelmien turvallisuutta ja eheyttä, ehkäistä hyökkäyksiä ja vähentää hyökkäysten vaikutuksia; tukee komissiota sen pyrkimyksissä esittää yrityksiä koskevat tietoverkkoturvallisuuden ja sertifiointijärjestelmien vähimmäisvaatimukset sekä tarjota oikeita aloitteita yksityisen sektorin turvallisuuden parantamiseksi tekemien ponnistelujen voimistamiseksi;

38. kehottaa komissiota ja jäsenvaltioiden hallituksia kannustamaan yksityissektoria ja kansalaisyhteiskunnan toimijoita sisällyttämään tietoverkon kriisinhallinta kriisinhallintasuunnitelmaansa ja riskiselvityksiinsä; kehottaa näitä myös valistamaan kaikkia henkilöstönsä jäseniä tietoverkkoturvallisuuden ja sen parantamisen perusteista;

39. kehottaa komissiota yhteistyössä jäsenvaltioiden ja asianomaisten virastojen ja elinten kanssa laatimaan puitteet ja välineet nopealle tiedonvaihtojärjestelmälle, jonka avulla voidaan varmistaa nimettömyys yksityiselle sektorille verkkoturvallisuuspoikkeamista ilmoitettaessa, mahdollistaa julkisten toimijoiden pysyminen jatkuvasti ajan tasalla ja antaa tarvittaessa apua;

40. tähdentää, että EU:n on helpotettava kilpailukykyisten ja innovatiivisten tietoverkkoturvallisuusmarkkinoiden kehitystä EU:ssa, jotta pk-yrityksillä olisi paremmat mahdollisuudet toimia tällä talouskasvua ja työpaikkojen luomista edistävällä alalla;

Kansainvälinen yhteistyö

41. kehottaa EUH:ta omaksumaan tietoverkkoturvallisuutta koskevan ennakoivan linjauksen ja ottamaan tietoturvallisuusnäkökulman huomioon kaikissa toimissaan ja etenkin niissä, jotka suuntautuvat kolmansiin maihin; kehottaa nopeuttamaan yhteistyötä ja tiedonvaihtoa, joka koskee tietoverkkoturvallisuusongelmien torjumista kolmansissa maissa;

42. painottaa, että EU:n kattavan tietoverkkoturvallisuusstrategian loppuun saattaminen on ennakkoedellytys sellaisen kansainvälisen tietoverkkoturvallisuusyhteistyön luomiselle, jota tarvitaan rajatylittävien tietoverkkouhkien torjumiseen;

43. kehottaa jäsenvaltioita, jotka eivät ole vielä allekirjoittaneet tai ratifioineet tietoverkkorikollisuutta koskevaa Euroopan neuvoston yleissopimusta (Budapestin yleissopimus), tekemään sen välittömästi; tukee komissiota ja EUH:ta niiden pyrkimyksissä edistää yleissopimusta ja sen arvoja kolmansissa maissa;

44. tiedostaa kansainvälisellä tasolla sovitun tietoverkkouhkia koskevan koordinoidun ratkaisun tarpeen; kehottaa sen vuoksi komissiota, EUH:ta ja jäsenvaltioita ottamaan johtavan aseman kaikilla sellaisilla foorumeilla ja erityisesti Yhdistyneissä kansakunnissa (YK), joilla pyritään saavuttamaan laajempi kansainvälinen yhteistyö ja lopullinen sopimus yhteisistä tietoverkon käyttönormeista, ja tukemaan myös kyberaseiden valvontaa koskevien sopimusten laatimiseen tähtäävää yhteistyötä;

45. kannustaa tietämyksen vaihtoon verkkoturvallisuuden alalla BRICS-maiden ja muiden nousevan talouden maiden kanssa, jotta voidaan tutkia, olisiko mahdollista löytää yhteisiä tapoja vastata lisääntyviin siviili- ja sotilaallisen tason tietoverkkorikoksiin, -uhkiin ja -hyökkäyksiin;

Torstai 22. marraskuuta 2012

46. kehottaa EUH:ta ja komissiota omaksumaan ennakoivan linjan alan kansainvälisissä foorumeissa ja järjestöissä ja erityisesti YK:ssa, Etyjissä, OECD:ssä ja Maailmanpankissa ja pyrkimään näin soveltamaan voimassa olevaa kansainvälistä lainsäädäntöä ja saavuttamaan yhteisymmärryksen tietoverkkoturvallisuutta ja -puolustusta koskevista vastuullisen valtion toimintatavoista koordinoimalla jäsenvaltioiden kantoja, jotta voidaan edistää tietoverkkoturvallisuutta ja -puolustusta koskevia EU:n ydinarvoja ja keskeisiä toimintaperiaatteita;

47. kehottaa neuvostoa ja komissiota korostamaan vuoropuhelussaan, suhteissaan ja yhteistyösopimuksissaan kolmansien maiden kanssa vähimmäisvaatimuksia, joiden avulla voidaan estää ja torjua tietoverkkorikollisuutta ja -hyökkäyksiä, ja painottamaan myös tietojärjestelmäturvallisuuden vähimmäisvaatimuksia, ja pyytää niitä toimimaan näin erityisesti sellaisten kolmansien maiden kanssa, joiden suunnitelmissa on tehdä yhteistyötä tai vaihtaa kokemuksia tekniikan alalla;

48. kehottaa komissiota tukemaan tarvittaessa kolmansia maita niiden pyrkimyksissä rakentaa omat tietoverkkoturvallisuutta ja -puolustusta koskevat valmiutensa;

Yhteistyö Naton kanssa

49. toteaa, että yhteisten arvojensa ja strategisten etujensa perusteella EU:lla ja Natolla on erityinen vastuu ja valmius puuttua lisääntyviin tietoverkkoturvallisuusongelmiin tehokkaammin ja tiiviissä yhteistyössä etsimällä täydentävyyksiä ilman päällekkäisyyksiä kuitenkin siten, että molemmat osapuolet täyttävät omat velvollisuutensa;

50. korostaa tarvetta keskittää ja jakaa voimavaroja käytännön tasolla ottaen huomioon EU:n ja Naton tietoverkkoturvallisuutta ja -puolustusta koskevan linjauksen täydentävyyden; korostaa, että tietoverkkoturvallisuutta ja -puolustusta koskevaa yhteistyötä on tiivistettävä suunnittelun, teknologian, koulutuksen ja välineiden osalta;

51. ottaa huomioon tarpeen kehittää puolustusvalmiuksia nykyisten toisiaan täydentävien toimien pohjalta ja kehottaa kaikkia tietoverkkoturvallisuuden ja -puolustuksen parissa EU:ssa toimivia elimiä tiivistämään käytännön yhteistyötään Naton kanssa, jotta voidaan vaihtaa kokemuksia ja oppia, miten EU:n järjestelmiä voidaan vahvistaa;

Yhteistyö Yhdysvaltojen kanssa

52. katsoo, että EU:n ja Yhdysvaltojen olisi lisättävä keskinäistä yhteistyötään, jonka avulla voidaan torjua tietoverkkohyökkäyksiä ja -rikoksia, sillä tämä asetettiin transatlanttisten suhteiden ensisijaiseksi tavoitteeksi Lissabonissa vuonna 2010 pidetyn EU:n ja Yhdysvaltojen huippukokouksen seurauksena;

53. suhtautuu myönteisesti marraskuussa 2010 pidetyssä EU:n ja Yhdysvaltojen huippukokouksessa toteutuneeseen EU:n ja Yhdysvaltojen verkkoturvallisuus- ja verkkorikollisuustyöryhmän perustamiseen ja tukee sen pyrkimyksiä sisällyttää internetin turvallisuutta koskevat kysymykset transatlanttiseen poliittiseen vuoropuheluun;

54. on tyytyväinen siihen, että komissio laatii Yhdysvaltojen kanssa EU:n ja Yhdysvaltojen verkkoturvallisuus- ja verkkorikollisuustyöryhmän alaisuudessa vuosiksi 2012/2013 yhteisen ohjelman ja etenemissuunnitelman yhteisiä tai yhteensovitettuja mannertenvälisiä verkkoturvallisuusharjoituksia varten; panee merkille ensimmäisen EU:n ja Yhdysvaltojen yhteisen verkkoturvallisuusharjoituksen (”Cyber Atlantic”), joka järjestettiin vuonna 2011;

55. korostaa, että Yhdysvaltojen ja EU:n, jotka ovat verkkoympäristön suurimpia tuottajia ja joissa on eniten verkonkäyttäjiä, on työskenneltävä yhdessä suojellakseen kansalaistensa tämän ympäristön käyttöön liittyviä oikeuksia ja vapauksia; korostaa, että kansallinen turvallisuus on tärkein tavoite ja että tietoverkkoympäristö on turvattava mutta sitä on myös suojeltava;

o

o o

56. kehottaa puhemiestä välittämään tämän päätöslauselman neuvostolle, komissiolle, korkealle edustajalle / varapuheenjohtajalle, EDA:lle, ENISAlle ja Natolle.