EUROOPAN PARLAMENTTI 2009 - 2014

Istuntoasiakirja

6.9.2013 B7-0386/2013

PÄÄTÖSLAUSELMAESITYS

komission julkilausuman johdosta

työjärjestyksen 110 artiklan 2 kohdan mukaisesti

Euroopan unionin kyberturvallisuussuunnitelmasta – avoin, turvallinen ja vakaa verkkoympäristö
(2013/2606(RSP))

Malcolm Harbour, Andreas Schwab
kansainvälisen kaupan valiokunnan puolesta
Elmar Brok, Tunne Kelam
ulkoasiainvaliokunnan puolesta

B7-0386/2013

Euroopan parlamentin päätöslauselman Euroopan unionin kyberturvallisuussuunnitelmasta – avoin, turvallinen ja vakaa verkkoympäristö (2013/2606(RSP))

Euroopan parlamentti, joka

– ottaa huomioon komission ja Euroopan unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan 7. helmikuuta 2013 antaman yhteisen tiedonannon ”Euroopan unionin kyberturvallisuussuunnitelma – avoin, turvallinen ja vakaa verkkoympäristö” (JOIN(2013)1),

– ottaa huomioon 7. helmikuuta 2013 annetun komission ehdotuksen direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa (COM(2013)0048),

– ottaa huomioon 19. toukokuuta 2010 annetun komission tiedonannon ”Euroopan digitaalistrategia” (COM(2010)0245) ja 18. joulukuuta 2012 annetun komission tiedonannon ”Euroopan digitaalistrategia – Euroopan kasvun vauhdittaminen digitaalisin keinoin” (COM(2012)0784),

– ottaa huomioon 27. syyskuuta 2012 annetun komission tiedonannon ”Pilvipalvelujen potentiaali käyttöön Euroopassa” (COM(2012)0529),

– ottaa huomioon komission 28. maaliskuuta 2013 antaman tiedonannon ”Rikostentorjunta digitaaliaikana: Euroopan verkkorikostorjuntakeskuksen perustaminen” (COM(2012)0140) ja neuvoston aiheesta 7. kesäkuuta 2012 esittämät päätelmät,

– ottaa huomioon tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2013/222/YOS korvaamisesta 12. elokuuta 2013 annetun Euroopan parlamentin ja neuvoston direktiivin 2005/40/EU[1],

– 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[2],

– ottaa huomioon lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta ja neuvoston puitepäätöksen 2004/68/YOS korvaamisesta 13. joulukuuta 2011 annetun Euroopan parlamentin ja neuvoston direktiivin 2011/92/EU[3],

– ottaa huomioon vapauden, turvallisuuden ja oikeuden aluetta koskevan Tukholman ohjelman[4], komission tiedonannon ”Vapauden, turvallisuuden ja oikeuden alueen toteuttaminen EU:n kansalaisten hyväksi – Toimintasuunnitelma Tukholman ohjelman

[1] EUVL L 218, 14.8.2013, s. 8.
[2] EUVL L 345, 23.12.2008, s. 75.
[3] EUVL L 335, 17.12.2011, s. 1.
[4] EUVL C 115, 4.5.2010, s. 1.

toteuttamiseksi” (COM(2010)0171) sekä komission tiedonannon ”EU:n sisäisen turvallisuuden strategian toteuttamissuunnitelma: viisi askelta kohti turvallisempaa Eurooppaa” (COM(2010)0673) sekä 22. toukokuuta 2012 antamansa päätöslauselman Euroopan unionin sisäisestä turvallisuusstrategiasta[1],

– ottaa huomioon komission ja korkean edustajan yhteisen ehdotuksen neuvoston päätökseksi järjestelyistä, joiden mukaisesti unioni panee täytäntöön yhteisvastuulausekkeen (JOIN/2012/039),

– ottaa huomioon muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjunnasta 28. toukokuuta 2001 tehdyn neuvoston puitepäätöksen 2001/413/YOS[2],

– ottaa huomioon 12. kesäkuuta 2012 antamansa päätöslauselman elintärkeiden tietoinfrastruktuureiden suojaamisesta – saavutukset ja seuraavat vaiheet: kohti maailmanlaajuista verkkoturvallisuutta[3] ja neuvoston 27. toukokuuta 2011 esittämät päätelmät komission tiedonannosta ”elintärkeiden tietoinfrastruktuureiden suojaamisesta ”Saavutukset ja seuraavat vaiheet: kohti maailmanlaajuista verkkoturvallisuutta” (COM(2011)0163),

– ottaa huomioon 11. joulukuuta 2012 antamansa päätöslauselman digitaalisten yhtenäismarkkinoiden toteuttamisesta[4],

– ottaa huomioon 22. marraskuuta 2012 antamansa päätöslauselman tietoverkkoturvallisuudesta ja -puolustuksesta[5],

– ottaa huomioon ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi Euroopan verkko- ja tietoturvavirastosta (ENISA) (COM(2010)521) 16. huhtikuuta 2013 antamansa lainsäädäntöpäätöslauselman, jolla se esitti kantansa ensimmäisessä käsittelyssä[6],

– ottaa huomioon 11. joulukuuta 2012 antamansa päätöslauselman digitaalisen vapauden strategiasta EU:n ulkopolitiikassa[7],

– ottaa huomioon 23. marraskuuta 2001 tehdyn Euroopan neuvoston yleissopimuksen tietoverkkorikollisuudesta,

– ottaa huomioon unionin kansainväliset velvoitteet ja etenkin palvelukaupan yleissopimuksen (GATS) mukaiset velvoitteet,

– ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklan ja Euroopan unionin perusoikeuskirjan ja etenkin sen 6, 8 ja 11 artiklan[8],

---

[1] Hyväksytyt tekstit, P7_TA(2012)0207.
[2] EUVL L 149, 2.6.2001, s. 1.
[3] Hyväksytyt tekstit, P7_TA(2012)0237.
[4] Hyväksytyt tekstit, P7_TA(2012)0468.
[5] Hyväksytyt tekstit, P7_TA(2012)0457.
[6] Hyväksytyt tekstit, P7_TA(2013)0103.
[7] Hyväksytyt tekstit, P7_TA(2012)0470.
[8] EUVL C 83, 30.3.2010, s. 389.

– ottaa huomioon käynnissä olevat Euroopan unionin ja Yhdysvaltojen väliset neuvottelut transatlanttisesta kauppa- ja investointikumppanuudesta,

– ottaa huomioon työjärjestyksen 110 artiklan 2 kohdan,

A. toteaa, että kasvavat tietoverkkohaasteet, jotka ovat yhä monimutkaisempia uhkia ja hyökkäyksiä, ovat suuri uhka jäsenvaltioiden turvallisuudelle, vakaudelle ja taloudelliselle hyvinvoinnille sekä yksityissektorille ja laajemmalle yhteisölle; katsoo, että yhteiskuntamme ja taloutemme suojaaminen on siksi jatkuvasti kehittyvä haaste;

B. katsoo, että tietoverkkojen ja tietoverkkoturvallisuuden pitää muodostaa yksi EU:n ja kunkin jäsenvaltion turvallisuus- ja puolustuspolitiikan strategisista pilareista; katsoo, että on hyvin tärkeää varmistaa, että tietoverkko pysyy avoimena ideoiden vapaalle vaihdolle, tiedon kululle ja itseilmaisulle;

C. katsoo, että sähköinen kaupankäynti ja verkkopalvelut ovat Internetin elinvoima ja että ne ovat ratkaisevia Eurooppa 2020 -strategian tavoitteille, sillä ne hyödyttävät sekä kansalaisia että yksityissektoria; katsoo, että unionin on tajuttava täysin internetin tuoma potentiaali ja mahdollisuudet yhtenäismarkkinoiden kehittämisessä edelleen, digitaaliset yhtenäismarkkinat mukaan lukien;

D. toteaa, että Euroopan unionin kyberturvallisuusstrategiaa koskevassa yhteisessä tiedonannossa hahmoteltuihin strategisiin pääasioihin kuuluvat tietoverkkojen kestävyyden saavuttaminen, tietoverkkorikosten vähentäminen, yhteiseen turvallisuus- ja puolustuspolitiikkaan (YTPP) liittyvien tietoverkkoja koskevan puolustuspolitiikan ja tietoverkkovalmiuksien kehittäminen sekä EU:n johdonmukaisen kansainvälisen tietoverkkopolitiikan kehittäminen;

E. toteaa, että unionin verkko- ja tietojärjestelmät ovat suuressa määrin liittyneet toisiinsa; katsoo, että internetin globaalin luonteen vuoksi monet verkkoihin ja tietoturvaan liittyvät vaaratilanteet ylittävät kansalliset rajat ja voivat heikentää sisämarkkinoiden toimintaa sekä kuluttajien digitaalisia yhtenäismarkkinoita kohtaan tuntemaa luottamusta;

F. toteaa, että verkkoturvallisuus unionissa ja muualla maailmassa on vain niin vahva kuin sen heikoin lenkki, ja häiriöt yhdellä alalla tai yhdessä jäsenvaltiossa vaikuttavat muihinkin aloihin ja jäsenvaltioihin, jolloin tästä aiheutuvat seuraukset vaikuttavat koko unionin talouteen;

G. panee merkille, että huhtikuuhun 2013 mennessä vain 13 jäsenvaltiota oli virallisesti hyväksynyt kansallisen verkkoturvallisuusstrategian; panee merkille, että jäsenvaltioiden välillä on edelleen perustavanlaatuisia eroja, jotka liittyvät niiden valmiuteen, turvallisuuteen, strategiseen kulttuuriin ja kykyyn kehittää ja toteuttaa kansallisia verkkoturvallisuusstrategioita, ja katsoo, että näitä eroja olisi arvioitava;

H. toteaa, että turvallisuuskulttuurin erot ja oikeudellisen kehyksen puute johtavat hajanaisuuteen ja ne ovat ensisijainen huolenaihe digitaalisilla yhtenäismarkkinoilla, toteaa, että tietoverkkoturvallisuutta koskevan yhtenäisen menettelyn puuttuminen vaarantaa vakavasti taloudellisen hyvinvoinnin sekä liiketoimien turvallisuuden, minkä vuoksi tarvitaan yhteisiä toimia ja entistä tiiviimpää yhteistyötä hallitusten ja

yksityissektorin sekä lakien täytäntöönpanosta ja tiedustelutoiminnasta vastaavien virastojen välillä;

I. toteaa, että tietoverkkorikollisuus on yhä kalliimmaksi käyvä kansainvälinen ongelma, joka maksaa Yhdistyneiden kansakuntien huume- ja rikollisuusviraston mukaan tällä hetkellä maailmantaloudelle vuosittain lähes 295 miljardia euroa;

J. toteaa, että teknistä kehitystä hyödyntävä kansainvälinen järjestäytynyt rikollisuus on siirtämässä toimintaansa tietoverkkoihin ja että tietoverkkorikollisuus on muuttamassa järjestäytyneen rikollisuuden ryhmien perinteistä rakennetta radikaalisti; toteaa tämän johtaneen siihen, että järjestäytynyt rikollisuus on vähemmän paikallista ja se käyttää entistä todennäköisemmin alueellisuutta ja kansallisten oikeusjärjestelmien eroja globaalilla tasolla;

K. toteaa, että toimivaltaisten viranomaisten harjoittamaa tietoverkkorikollisuuden tutkintaa haittaavat edelleen monet esteet, kuten rahanpesun mahdollistavan "virtuaalivaluutan" käyttö tietoverkossa käytävässä kaupassa, alueellisuuteen ja oikeusjärjestelmien rajoihin liittyvät kysymykset, riittämätön kapasiteetti tiedustelutietojen vaihtoon, koulutetun henkilöstön puute sekä epäyhtenäinen yhteistyö muiden sidosryhmien kanssa;

L. toteaa tekniikan muodostavan tietoverkkojen kehittämisen perustan ja pitää jatkuvaa mukautumista teknologisiin muutoksiin keskeisenä, jos EU:n tietoverkkojen kestävyyttä ja turvallisuutta halutaan parantaa; katsoo, että on ryhdyttävä toimiin sen varmistamiseksi, että lainsäädäntö pysyy uusimman teknisen kehityksen tasolla niin, että tietoverkkorikolliset voidaan tehokkaasti tunnistaa ja asettaa syytteeseen ja tietoverkkorikosten uhreja voidaan suojella;

1. pitää myönteisenä yhteistä tiedonantoa, joka koskee Euroopan unionin kyberturvallisuusstrategiaa ja ehdotusta direktiiviksi toimista, joilla varmistetaan verkko- ja tietoturvan korkea taso koko unionissa;

2. korostaa internetin ja tietoverkkojen keskeistä ja yhä kasvavaa merkitystä poliittisten, taloudellisen ja yhteiskuntaan liittyvän tietojen vaihdon yhteydessä paitsi unionissa myös suhteessa muihin toimijoihin koko maailmassa;

3. korostaa, että on laadittava strateginen tiedonanto, jossa käsitellään EU:n kyberturvallisuuspolitiikkaa, tietoverkkojen kriisitilanteita, strategisia tarkasteluja, julkisen ja yksityisen sektorin yhteistyötä sekä yleisölle annettavia varoituksia ja suosituksia;

4. muistuttaa, että tarvitaan verkko- ja tietoturvan korkeaa tasoa, jotta voidaan ylläpitää yhteiskunnan asianmukaisen toiminnan edellyttämiä palveluita, mutta niitä edellyttää myös kansalaisten fyysisen koskemattomuuden turvaaminen, sillä niiden avulla voidaan parantaa keskeisten infrastruktuurien tehokkuutta ja turvallista toimintaa; korostaa, että samalla, kun on käsiteltävä verkko- ja tietoturvaa, myös fyysisen turvallisuuden parantaminen on tärkeä kysymys; korostaa, että infrastruktuurin pitäisi olla kestävää sekä tahallisten että tahattomien häiriöiden suhteen; korostaa, että siksi kyberturvallisuutta koskevassa strategiassa pitäisi keskittyä entistä enemmän tahattomien järjestelmäongelmien yleisiin syihin;

5. kehottaa jälleen jäsenvaltioita ottamaan käyttöön kansallisia kyberturvallisuusstrategioita, jotka kattavat tekniikkaan, koordinointiin, henkilöstöresursseihin ja annettavaan rahoitukseen liittyvät näkökohdat ja joihin sisältyy yksityiskohtaisia sääntöjä yksityissektorin tuista ja vastuista, jotta voidaan varmistaa yksityissektorin osallistuminen mahdollisimman nopeasti; kehottaa myös toteuttamaan kattavia riskinhallintamenettelyjä ja turvaamaan sääntely-ympäristön;

6. toteaa, että vain unionin toimielinten ja jäsenvaltioiden yhdistetty johtajuus ja poliittinen omistajuus mahdollistavat verkko- ja tietoturvan korkean tason koko unionissa ja edistävät näin yhtenäismarkkinoiden varmaa ja häiriötöntä toimintaa;

7. korostaa, että unionin kyberturvallisuutta koskevan politiikan avulla olisi luotava turvallinen ja luotettava digitaalinen ympäristö, jonka perustana ovat ja jolla pyritään turvaamaan ja säilyttämään verkossa vapaudet ja perusoikeudet noudattaen EU:n perusoikeuskirjan 16 artiklaa ja erityisesti yksityisyyttä ja tietosuojaa koskevia oikeuksia; katsoo, että erityistä huomiota pitäisi kiinnittää lasten suojelemiseen verkossa;

8. kehottaa jäsenvaltioita ja komissiota toteuttamaan kaikki tarvittavat toimet, jotta voitaisiin toteuttaa koulutusohjelmia, joilla edistetään ja parannetaan Euroopan kansalaisten tietämystä, taitoja ja koulutusta erityisesti liittyen henkilökohtaiseen turvallisuuteen osana digitaalisen lukutaidon ohjelmaa jo nuoresta iästä lähtien; pitää myönteisenä aloitetta Euroopan kyberturvallisuuskuukauden järjestämisestä ENISAn tuella ja yhteistyössä julkisten viranomaisten sekä yksityissektorin kanssa, jotta voidaan parantaa tietämystä verkko- ja tietojärjestelmien suojaamiseen liittyvistä haasteista;

9. katsoo, että kyberturvallisuutta koskeva koulutus parantaa Euroopan yhteiskunnan tietämystä kyberuhkista, mikä edistää tietoverkkojen vastuullista käyttöä ja auttaa parantamaan tietoverkkoja koskevaa yleistä tietämystä; panee merkille Europolin ja sen uuden tietoverkkorikollisuutta käsittelevän eurooppalaisen keskuksen (EC3) roolin koulutustoimien tarjoamisessa EU:n tasolla liittyen kansainvälisen oikeudellisen yhteistyön välineiden käyttöön ja oikeuden täytäntöönpanoon tietoverkkorikosten erilaisten näkökohtien osalta;

10. toistaa, että on annettava teknisiä neuvoja ja oikeudellista tietoa sekä perustettava ohjelmia, jotka liittyvät tietoverkkorikosten ennaltaehkäisyyn ja torjumiseen; kehottaa kouluttamaan tietoverkkoinsinöörejä, jotka erikoistuvat keskeisten infrastruktuurien ja tietojärjestelmien suojaamiseen, ja kehottaa kouluttamaan myös liikenteen ohjausjärjestelmien ja liikenteenhallintakeskusten käyttäjiä; korostaa, että on otettava käyttöön säännöllisiä kyberturvallisuutta koskevia koulutusohjelmia julkisen sektorin henkilöstölle kaikilla tasoilla;

11. toistaa, että on noudatettava varovaisuutta rajoitettaessa kansalaisten mahdollisuuksia viestintä- ja tietotekniikan välineiden käyttöön; korostaa, että jäsenvaltioiden ei pitäisi koskaan vaarantaa kansalaisten oikeuksia ja vapauksia kehitettäessä vastatoimia kyberuhkiin ja -hyökkäyksiin; katsoo, että niillä pitäisi olla riittävät lainsäädännölliset välineet tietoverkkoihin liittyvien siviili- ja sotilaallisen tason vaaratilanteiden erottamiseksi toisistaan;

12. katsoo, että kyberturvallisuutta koskeva sääntely pitää suunnata riskien mukaisesti ja siinä

pitää keskittyä kriittiseen infrastruktuuriin, jonka asianmukainen toiminta on tärkeä yleiseen etuun liittyvä tekijä; katsoo, että perustana on sovellettava alalla jo olemassa olevia markkinapohjaisia toimia, joilla verkkojen kestävyys taataan; korostaa toiminnallisen tason yhteistyön merkitystä pyrittäessä entistä tehokkaampaan kyberuhkia koskevaan tiedonvaihtoon julkisten viranomaisten ja yksityissektorin välillä sekä unionin että kansallisella tasolla tarkoituksena taata verkko- ja tietoturva niin, että luodaan molemminpuolinen luottamus, arvo ja sitoutuminen sekä vaihtoon liittyvä asiantuntemus; katsoo, että julkisen ja yksityisen sektorin kumppanuuksien pitäisi perustua verkkojen ja tekniikan neutraaliuteen ja niissä pitäisi keskittyä sellaisten ongelmien käsittelyyn, joilla on merkittävä julkinen vaikutus; kehottaa komissiota kannustamaan kaikkia asianomaisia markkinoiden toimijoita entistä suurempaan valppauteen ja yhteistyöhön, jotta voidaan suojata muita toimijoita niiden palveluille aiheutuvilta vahingoilta;

13. katsoo, että kyberturvallisuuteen liittyvien vaaratilanteiden havaitseminen ja niistä ilmoittaminen ovat keskeisellä sijalla edistettäessä tietoverkkojen kestävyyttä unionissa; katsoo, että olisi määritettävä suhteellisuutta ja tarvittavaa tietojen julkistamista koskevat vaatimukset, jotta kansallisille viranomaisille voidaan ilmoittaa tapauksista, joihin liittyy merkittäviä tietoturvan loukkauksia, mikä mahdollistaa kyberrikosten seurannan parantamisen ja edistää tietämyksen parantamista kaikilla tasoilla;

14. kehottaa komissiota ja muita toimijoita ottamaan käyttöön kyberturvallisuutta ja tietoverkkojen kestävyyttä koskevia toimia, jotka käsittävät taloudellisia kannustimia kyberturvallisuuden ja tietoverkkojen kestävyyden korkean tason edistämiseksi;

Tietoverkkojen kestävyys

15. toteaa, että eri aloilla ja jäsenvaltioilla on erilainen valmius- ja taitotaso ja että se estää luottamukseen perustuvan yhteistyön kehittämistä ja heikentää yhtenäismarkkinoiden toimintaa;

16. katsoo, että pk-yrityksiä koskevissa vaatimuksissa pitäisi soveltaa suhteellista ja riskiperusteista menettelyä;

17. vaatii kehittämään keskeisiin infrastruktuureihin liittyvää tietoverkkojen kestävyyttä ja muistuttaa, että tulevissa yhteisvastuulausekkeen (SEUT-sopimuksen 222 artikla) toteuttamista koskevissa menettelyissä olisi otettava huomioon jäsenvaltioon kohdistuva kyberisku; kehottaa komissiota ja korkeaa edustajaa ottamaan tämän riskin huomioon uhkia ja riskejä koskevissa yhteisissä kertomuksissaan, joita esitetään vuodesta 2015 alkaen;

18. korostaa, että erityisesti keskeisten palveluiden loukkaamattomuuden, käytettävyyden ja luottamuksellisuuden takaamiseksi keskeisten infrastruktuurien tunnistamisen ja luokittelun on oltava ajan tasalla, ja on asetettava niiden verkko- ja tietojärjestelmien turvallisuutta koskevat vähimmäisvaatimukset;

19. toteaa, että direktiiviehdotuksessa toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa säädetään tällaisista tietoyhteiskunnan palveluita tarjoavien tahojen ja kriittisten infrastruktuurien käyttäjien turvallisuuden vähimmäisvaatimuksista;

20. kehottaa jäsenvaltioita ja unionia toteuttamaan nopeille ja kaksisuuntaisille tiedonvaihtojärjestelmille riittävät kehykset, jotka mahdollistavat anonyymiyden yksityissektorille ja pitävät julkisen sektorin jatkuvasti ajan tasalla ja antavat tarvittaessa apua yksityissektorille;

21. pitää myönteisenä komission ilmoitusta kyberturvallisuuteen liittyvän riskinhallintakulttuurin perustamisesta ja kehottaa jäsenvaltioita ja unionin toimielimiä sisällyttämään kyberkriisien hallinnan nopeasti niiden kriisinhallintasuunnitelmiin ja riskianalyyseihin; kehottaa lisäksi jäsenvaltioiden hallituksia ja komissiota kannustamaan yksityistä sektoria sisällyttämään kyberkriisien hallinnan niiden hallintasuunnitelmiin ja riskianalyyseihin ja kehottaa niitä antamaan henkilöstölleen kyberturvallisuutta koskevaa koulutusta;

22. kehottaa kaikkia jäsenvaltioita ja unionin toimielimiä perustamaan hyvin toimivien tietotekniikan CERT-kriisiryhmien verkon, joka on toiminnassa joka päivä 24 tuntia vuorokaudessa; korostaa, että kansallisten CERT-ryhmien olisi oltava osa tehokasta verkkoa, jossa asiaan liittyviä tietoja vaihdetaan noudattaen asianmukaisia luottamusta ja luottamuksellisuutta koskevia normeja; toteaa, että CERT-ryhmät ja muut asianomaiset turvallisuusryhmät yhteen kokoavat aloitteet voivat olla hyödyllisiä välineitä kehitettäessä rajat ylittävää ja eri alojen välistä luottamusta; pitää kyberrikosten torjunnassa tärkeänä tehokasta ja toimivaa yhteistyötä CERT-ryhmien ja lakien täytäntöönpanosta vastaavien virastojen välillä;

23. tukee ENISAa sen verkko- ja tietoturvallisuuteen liittyvissä tehtävissä etenkin annettaessa ohjausta ja neuvoja jäsenvaltioille ja tuettaessa parhaiden käytäntöjen vaihtoa ja luottamuksen ilmapiirin kehittämistä;

24. korostaa, että alan on pantava täytäntöön kyberturvallisuutta koskevia toiminnallisia vaatimuksia sellaisten tieto- ja viestintätekniikan tuotteiden koko arvoketjussa, joita käytetään liikenneverkoissa ja tietojärjestelmissä, jotta voidaan suorittaa asianmukaista riskien arviointia, ottaa käyttöön turvanormeja ja -ratkaisuja ja jotta voidaan kehittää parhaita käytäntöjä ja tietojen vaihtoa liikennejärjestelmien kyberturvallisuuden varmistamiseksi;

Teolliset ja teknologiset resurssit

25. katsoo, että verkko- ja tietoturvan korkea taso on keskeisellä sijalla parannettaessa sekä turvallisuusratkaisujen toimittajien että niiden käyttäjien kilpailukykyä unionissa; katsoo, että unionin tietotekniikka-alalla on merkittävää vielä hyödyntämätöntä potentiaalia, mutta yksityisillä ja julkisilla käyttäjillä sekä yrityksillä ei usein vieläkään ole tietoja kustannuksista ja hyödyistä, joita kyberturvallisuuteen investoimisesta seuraa, minkä vuoksi ne ovat haavoittuvia haitallisten kyberuhkien suhteen; korostaa, että CERT-ryhmien toteutus on tässä suhteessa merkityksellinen tekijä;

26. katsoo, että kyberturvallisuuteen liittyvien ratkaisujen vahva tarjonta ja kysyntä edellyttävät tieto- ja viestintätekniikasta vastaavilta viranomaisilta riittäviä investointeja akateemisiin resursseihin, tutkimukseen ja kehittämiseen sekä tietämyksen ja kapasiteetin lisäämiseen, jotta voidaan edistää innovointia ja saada aikaan riittävä tietämys verkko- ja tietoturvaan liittyvistä riskeistä ja siirtyä kohti yhtenäistä eurooppalaista turvallisuusalaa;

27. kehottaa unionin toimielimiä ja jäsenvaltioita toteuttamaan tarvittavat toimet sellaisten ”kyberturvallisuuden yhtenäismarkkinoiden” luomiseksi, joilla käyttäjät ja toimittajat voivat hyödyntää parhaalla tavalla tarjolla olevia innovaatioita, synergiavaikutuksia ja yhdistettyä asiantuntemusta ja joille pk-yritykset voivat päästä;

28. kehottaa jäsenvaltioita harkitsemaan yhteisiä investointeja Euroopan kyberturvallisuusalalle samaan tapaan kuin on tehty muillakin aloilla, kuten ilmailualalla;

Kyberrikollisuus

29. katsoo, että tietoverkoissa tapahtuvat rikokset voivat olla yhteiskuntien hyvinvoinnin kannalta yhtä haitallisia kuin fyysisessä ympäristössä tapahtuvat rikokset ja että tällaiset rikosten muodot usein vahvistavat toisiaan, kuten voidaan havaita esimerkiksi lasten seksuaalisen hyväksikäytön, järjestäytyneen rikollisuuden ja rahanpesun yhteydessä;

30. toteaa, että joissakin tapauksissa laillinen ja laiton liiketoiminta ovat yhteydessä toisiinsa; korostaa, että terrorismin ja vakavan järjestäytyneen rikollisuuden rahoituksen välillä on tärkeä internetin mahdollistama yhteys; korostaa, että yleisö on saatava tietoiseksi vakavuudesta, joka liittyy kyberrikollisuuteen osallistumiseen, ja siitä, että usein ensi näkemältä ”sosiaalisesti hyväksyttävät” rikokset, kuten elokuvien laiton lataaminen, voivat usein tuoda suuria summia kansainvälisille rikollisjärjestöille;

31. on komission kanssa samaa mieltä siitä, että verkkojen ulkopuolella sovellettavat normit ja periaatteet pätevät myös verkossa, minkä vuoksi kyberrikollisuuden torjumista on tehostettava ajantasaisella lainsäädännöllä ja toiminnallisilla valmiuksilla;

32. katsoo, että kyberrikollisuuden rajattoman luonteen vuoksi tarvitaan erityisesti yhteisiä ponnistuksia ja tarjottavaa asiantuntemusta unionin tasolla yksittäisten jäsenvaltioiden tason yläpuolella ja että Eurojustin, Europolin, Euroopan verkkorikostorjuntakeskuksen (EC3), CERT-ryhmien ja yliopistojen sekä tutkimuskeskusten on siksi saatava riittäviä resursseja, jotta ne voivat toimia asianmukaisella tavalla asiantuntemuksen, yhteistyön ja tiedonvaihdon keskuksina;

33. pitää erittäin hyvänä Euroopan verkkorikostorjuntakeskuksen perustamista ja kannustaa kehittämään tätä keskusta ja sen tärkeää roolia tietojen ja asiantuntemuksen nopeassa ja tehokkaassa vaihtamisessa rajojen yli, jotta tuetaan verkkorikollisuuden estämistä, havaitsemista ja tutkintaa;

34. kehottaa jäsenvaltioita varmistamaan, että kansalaiset voivat helposti saada tietoa verkkouhkista ja niiden torjunnasta; katsoo, että tällaisten ohjeiden pitäisi sisältää tietoja siitä, miten käyttäjät voivat suojella yksityisyyttään internetissä, miten havaita verkkohoukuttelu ja ilmoittaa siitä, miten asentaa ohjelmia ja palomuureja, miten käyttää tunnussanoja ja miten havaita verkkourkinta, sivustoharhautukset ja muut hyökkäykset;

35. vaatii, että jäsenvaltiot, jotka eivät ole vielä ratifioineet tietoverkkorikollisuutta koskevaa Euroopan neuvoston Budapestin yleissopimusta, tekevät niin viipymättä; pitää myönteisenä Euroopan neuvoston ajatuksia tarpeesta päivittää yleissopimusta teknisen kehityksen mukaisesti, jotta voidaan taata jatkossakin sen tehokkuus verkkorikollisuuden käsittelyssä; kehottaa komissiota ja jäsenvaltioita osallistumaan asiaa koskevaan

keskusteluun; kannustaa toimiin, joilla edistetään yleissopimuksen ratifiointia muissa maissa, ja kehottaa komissiota edistämään sitä aktiivisesti unionin ulkopuolella;

Kyberpuolustus

36. korostaa, että kyberhaasteet, -uhkat ja -hyökkäykset vaarantavat jäsenvaltioiden puolustukseen ja kansalliseen turvallisuuteen liittyviä etuja ja että siviilitoimilla ja sotilaallisella menettelyllä keskeisen infrastruktuurin suojaamisessa olisi maksimoitava kummankin tahon saama hyöty niin, että pyritään saamaan aikaan synergiavaikutuksia;

37. kehottaa siksi jäsenvaltioita tehostamaan yhteistyötään Euroopan puolustusviraston kanssa, jotta voidaan kehittää kyberpuolustusvalmiuksia koskevia ehdotuksia ja aloitteita viimeaikaisten aloitteiden ja hankkeiden pohjalta; korostaa tarvetta lisätä tutkimusta ja kehittämistä myös resurssien yhdistämisen ja jakamisen avulla;

38. toistaa, että EU:n kattavassa kyberturvallisuutta koskevassa strategiassa olisi otettava huomioon olemassa olevien virastojen ja elinten tuoma lisäarvo sekä sellaisista jäsenvaltioista saadut hyvät käytännöt, jotka ovat jo ottaneet käyttöön omia kansallisia kyberturvallisuusstrategioita;

39. kehottaa varapuheenjohtajaa / korkeaa edustajaa ottamaan kyberkriisien hallinnan mukaan kriisinhallintasuunnitelmiin ja korostaa, että jäsenvaltioiden on yhteistyössä Euroopan puolustusviraston kanssa kehitettävä suunnitelmia YTPP-tehtävien ja -toimien suojaamiseksi kyberhyökkäyksiltä; kehottaa niitä kokoamaan yhteen eurooppalaiset kyberpuolustusjoukot;

40. korostaa kyberturvallisuuteen liittyvää hyvää käytännön yhteistyötä NATOn kanssa ja tarvetta tehostaa yhteistyötä etenkin tekemällä tiivistä yhteistyötä suunnittelun, tekniikan, koulutuksen ja välineiden suhteen;

41. kehottaa unionia pyrkimään vaihdon aikaansaamiseen kansainvälisten kumppanien kanssa, NATO mukaan lukien, ja kehottaa tunnistamaan yhteistyön aloja, välttämään päällekkäisyyksiä ja pyrkimään toiminnan täydentävyyteen mahdollisuuksien mukaan;

Kansainvälinen politiikka

42. katsoo, että kansainvälisellä yhteistyöllä ja vuoropuhelulla on keskeinen rooli luotaessa luottamusta ja avoimuutta ja edistettäessä korkeatasoista verkostoitumista ja tiedonvaihtoa maailmanlaajuisesti; kehottaa siksi komissiota ja Euroopan ulkosuhdehallintoa perustamaan kyberdiplomatiaryhmän, jonka tehtäviin kuuluu vuoropuhelun edistäminen samanmielisten maiden ja organisaatioiden kanssa; kehottaa EU:ta osallistumaan entistä aktiivisemmin monenlaisiin kyberturvallisuutta käsitteleviin kansainvälisiin korkean tason konferensseihin;

43. katsoo, että on saatava aikaan tasapaino toistensa kanssa kilpailevien tavoitteiden kanssa, joita ovat tiedon rajat ylittävä siirtäminen, tietoturva ja kyberturvallisuus, unionin kansainvälisten velvoitteiden ja erityisesti palvelukaupan yleissopimuksen (GATS) mukaisesti;

44. kehottaa varapuheenjohtajaa / korkeaa edustajaa valtavirtaistamaan kyberturvallisuuteen liittyvän ulottuvuuden EU:n ulkoisissa toimissa ja erityisesti suhteessa kolmansiin maihin, jotta voidaan tehostaa kyberturvallisuuden käsittelyyn liittyvää yhteistyötä sekä kokemusten ja tietojen vaihtoa;

45. kehottaa unionia pyrkimään vaihdon aikaansaamiseen kansainvälisten kumppanien kanssa, jotta voidaan tunnistaa yhteistyön aloja, välttää päällekkäisyyksiä ja pyrkiä toiminnan täydentävyyteen mahdollisuuksien mukaan; kehottaa varapuheenjohtajaa / korkeaa edustajaa ja komissiota toimimaan aktiivisesti kansainvälisissä organisaatioissa ja koordinoimaan jäsenvaltojen kantoja siihen, miten kyberalalla voidaan edistää ratkaisuja ja menettelyjä tehokkaasti;

46. katsoo, että pitäisi pyrkiä varmistamaan, että olemassa olevat kansainväliset oikeudelliset välineet ja erityisesti kyberrikollisuutta koskeva Euroopan neuvoston yleissopimus pannaan täyttöön tietoverkoissa; katsoo siksi, että tällä hetkellä ei tarvitse luoda uusia oikeudellisia välineitä kansainvälisellä tasolla; pitää kuitenkin myönteisenä kansainvälistä yhteistyötä, jolla pyritään kehittämään tietoverkossa toimimista koskevia normeja tukemaan oikeusvaltioperiaatteen toteutumista tietoverkoissa; katsoo, että olisi harkittava nykyisten oikeudellisten välineiden päivittämistä teknisen kehityksen mukaisesti; katsoo, että lainsäädäntöjärjestelmiin liittyvät kysymykset edellyttävät perinpohjaista keskustelua oikeudellisesta yhteistyöstä ja syytteeseenasettamisesta rajat ylittävissä rikostapauksissa;

47. katsoo erityisesti, että EU:n ja Yhdysvaltojen välisen kyberturvallisuutta ja kyberrikoksia käsittelevän työryhmän pitäisi olla väline, jonka avulla EU ja Yhdysvallat vaihtavat tarpeen mukaan kyberturvallisuutta koskevia parhaita käytäntöjä; panee tässä yhteydessä merkille, että kyberturvallisuuteen liittyvät alat, kuten verkko- ja tietojärjestelmien turvallisesta toiminnasta riippuvaiset palvelut, sisältyvät transatlanttista kauppa- ja investointikumppanuutta käsitteleviin tuleviin neuvotteluihin;

48. toteaa, että kyberturvallisuuteen liittyvät taidot ja kyky estää, havaita ja tehokkaasti vastustaa uhkia ja vihamielisiä hyökkäyksiä eivät jakaudu maailmassa tasaisesti; korostaa, että toimet tietoverkkojen kestävyyden parantamiseksi ja tietoverkkouhkien torjumiseksi eivät saa rajoittua samanmielisiin kumppaneihin, vaan niiden yhteydessä olisi käsiteltävä myös alueita, joiden kapasiteetti, tekninen infrastruktuuri ja oikeudelliset kehykset ovat vähemmän kehittyneitä; katsoo, että CERT-ryhmien koordinointi on tässä suhteessa keskeisellä sijalla; kehottaa komissiota edistämään ja tarvittaessa avustamaan sopivin keinoin kolmansia maita niiden pyrkimyksissä kehittää omia tietoverkkoturvallisuutta koskevia valmiuksiaan;

Täytäntöönpano

49. kehottaa arvioimaan säännöllisesti kansallisten kyberturvallisuusstrategioiden tehokkuutta korkeimmalla poliittisella tasolla, jotta voidaan varmistaa mukautuminen uusiin globaaleihin uhkiin ja taata kyberturvallisuuden samanlainen taso eri jäsenvaltioissa;

50. pyytää komissiota laatimaan selkeän etenemissuunnitelma, jossa määritetään aikataulu kyberturvallisuusstrategiaan liittyvien unionin tason tavoitteiden saavuttamiselle sekä niiden arvioinnille; kehottaa jäsenvaltioita sopimaan samanlaisesta aikataulusta tähän

strategiaan sisältyville kansallisille toimille;

51. pyytää komissiolta, jäsenvaltioilta, Europolilta, vasta perustetulta Euroopan verkkorikostorjuntakeskukselta, Eurojustilta ja ENISAlta säännöllisiä kertomuksia, joissa arvioidaan kehitystä kyberturvallisuusstrategiassa asetettujen tavoitteiden saavuttamisessa sekä esitetään keskeisiä toimintaindikaattoreita, joilla mitataan toteuttamisessa saavutettua kehitystä;

52. kehottaa puhemiestä välittämään tämän päätöslauselman neuvostolle, komissiolle, jäsenvaltioiden hallituksille ja parlamenteille, Europolille, Eurojustille sekä Euroopan neuvostolle.