EUROOPAN KOMISSIO

EUROOPAN UNIONIN
ULKOASIOIDEN
JA TURVALLISUUSPOLITIIKAN
KORKEA EDUSTAJA

Bryssel 7.2.2013
JOIN(2013) 1 final

YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE

Euroopan unionin kyberturvallisuusstrategia:

Avoin, turvallinen ja vakaa verkkoympäristö

YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE

Euroopan unionin kyberturvallisuusstrategia:

Avoin, turvallinen ja vakaa verkkoympäristö

1. JOHDANTO

1.1. Tausta

Internetillä ja laajemminkin koko verkkotoimintaympäristöllä on ollut viimeisten kahden vuosikymmenen aikana valtava vaikutus yhteiskunnan kaikkiin osa-alueisiin. Arjen sujuvuus, perusoikeuksien toteutuminen, sosiaalinen vuorovaikutus ja talouden toiminta ovat kaikki riippuvaisia tieto- ja viestintätekniikan saumattomasta toimivuudesta. Avoin ja vapaa verkkoympäristö on edistänyt poliittista ja yhteiskunnallista osallisuutta koko maailmassa: se on murtanut muureja maiden, yhteisöjen ja kansalaisten väliltä ja mahdollistanut vuorovaikutuksen ja tiedon- ja ajatustenvaihdon koko maailman laajuisesti, tarjonnut foorumin ilmaisunvapaudelle ja perusoikeuksien käytölle sekä valtaistanut ihmisiä pyrkimyksissä kohti demokraattisia ja oikeudenmukaisempia yhteiskuntia. Tämä näkyi erityisen selvästi ns. arabikevään aikana.

Jotta verkko säilyisi avoimena ja vapaana, verkkotoiminnassa olisi sovellettava samoja normeja, periaatteita ja arvoja, joita EU:ssa noudatetaan reaalimaailmankin puolella. Perusoikeuksia, demokratiaa ja oikeusvaltioperiaatetta on suojeltava myös kyberavaruudessa. Vapautemme ja hyvinvointimme on enenevässä määrin sidoksissa vakaaseen ja innovatiiviseen internetiin, joka jatkaa kukoistustaan, jos yksityisen sektorin innovaatiot ja kansalaisyhteiskunta toimivat sen kasvun vetureina. Verkkomaailman vapaus edellyttää kuitenkin myös turvallisuutta ja suojautumista. Verkko olisi suojattava tietoturvapoikkeamilta, ilkivaltaiselta toiminnalta ja väärinkäytöksiltä. Hallituksilla on merkittävä rooli vapaan ja turvallisen verkkoympäristön turvaamisessa. Niillä on useita tehtäviä: saatavuuden ja avoimuuden varmistaminen, perusoikeuksien noudattaminen ja suojelu verkossa sekä internetin luotettavuuden ja yhteentoimivuuden ylläpitäminen. Merkittävä osa verkkoympäristöstä on kuitenkin yksityisen sektorin omistuksessa ja käytössä, joten tämän alan aloitteiden on onnistuakseen tunnustettava myös yksityisten toimijoiden johtava rooli.

Tieto- ja viestintäteknologiasta on tullut talouskasvumme selkäranka ja kriittinen voimavara, josta kaikki talouden alat ovat riippuvaisia. Se on nyt perustana monimutkaisissa järjestelmissä, jotka pitävät taloutemme pyörät pyörimässä avainaloilla, kuten rahoitusalalla, terveydenhuollossa, energiahuollossa ja liikenteessä. Monet liiketoimintamallit rakentuvat internetin keskeytymättömälle saatavuudelle ja tietojärjestelmien sujuvalle toiminnalle.

Luomalla toimivat digitaaliset sisämarkkinat Eurooppa voisi korottaa bruttokansantuotettaan lähes 500 miljardilla eurolla vuodessa[1] eli keskimäärin 1000 eurolla asukasta kohti. Jotta uudet verkottuneet teknologiat, kuten verkkomaksujärjestelmät, pilvipalvelut ja koneiden väliset tiedonsiirtoratkaisut (M2M)[2], menestyisivät kansalaisten on voitava luottaa niihin.

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf.

[2] Esimerkiksi kasveihin istutettavat anturit, jotka ilmoittavat kastelujärjestelmälle kastelutarpeesta.

Vuonna 2012 tehty eurobarometrikysely[3] osoitti kuitenkin, että lähes kolmannes eurooppalaisista ei luota internetiin pankkiasioinnissa tai kauppapaikkana. Ylivoimainen enemmistö ilmoitti myös välttävänsä tietoturvaepäilysten vuoksi henkilötietojen antamista verkossa. EU:ssa useampi kuin joka kymmenes internetin käyttäjä on jo joutunut verkkopetoksen uhriksi.

Viime vuosina on nähty, että vaikka digitaalimaailma tarjoaa valtavia hyötyjä, se on myös haavoittuvainen. Kyberturvallisuuspoikkeamat[4], niin tahalliset kuin vahingotkin, ovat lisääntymässä hälyttävää tahtia ja ne voisivat häiritä keskeisten, itsestäänselvyyksinä pitämiemme palvelujen, kuten vesihuollon, terveydenhuollon, sähköntarjonnan ja matkaviestinnän, tarjontaa. Uhkia aiheutuu monista lähteistä: ne voivat esimerkiksi olla rikolliseen toimintaan tähtääviä, tarkoitusperiltään poliittisia tai ne voivat olla terroritekoja tai valtioiden rahoittamia hyökkäyksiä tai aiheutua luonnonkatastrofeista tai tahattomista virheistä.

EU:n talous kärsii jo nyt yksityiseen sektoriin ja yksityishenkilöihin kohdistuvasta verkkorikollisesta toiminnasta[5]. Verkkorikolliset käyttävät yhä kehittyneempiä menetelmiä murtautuakseen tietojärjestelmiin, anastaakseen kriittistä dataa tai kiristääkseen yrityksiä. Verkossa tapahtuvan teollisuusvakoilun ja valtiorahoitteisen toiminnan lisääntyminen muodostaa uuden uhkatyypin EU:n hallituksille ja yrityksille.

EU:n ulkopuolisissa maissa hallitukset voivat myös väärinkäyttää verkkoa omien kansalaistensa tarkkailuun ja valvontaan. EU voi pyrkiä parantamaan tilannetta edistämällä verkon vapautta ja varmistamalla, että perusoikeuksia kunnioitetaan verkkoympäristössä.

Kaikki nämä tekijät ovat johtaneet siihen, että hallitukset ympäri maailman ovat ryhtyneet laatimaan kyberturvallisuusstrategioita ja nostaneet verkkoympäristön yhä tärkeämmäksi kansainväliseksi kysymykseksi. EU:n on nyt tullut aika terävöittää toimiaan tällä alalla. Tässä komission sekä unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan, jäljempänä (jäljempänä "korkea edustaja"), ehdotuksessa Euroopan unionin kyberturvallisuusstrategiaksi hahmotellaan EU:n visiota tällä alalla, selvennetään rooleja ja vastuita sekä määritellään tarvittavat toimet, joilla pyritään kansalaisten oikeuksien vahvaan ja tulokselliseen suojaamiseen ja edistämiseen niin, että EU:n verkkoympäristöstä tulisi maailman turvallisin.

1.2. Kyberturvallisuuden periaatteet

Rajattomasta ja monikerroksisesta internetistä on tullut yksi voimakkaimmista välineistä, jotka edistävät globaalia kehitystä ilman valtioiden valvontaa tai sääntelyä. Yksityisen sektorin olisi edelleenkin oltava johtavassa roolissa internetin rakentamisessa ja jokapäiväisessä hallinnossa, mutta läpinäkyvyyteen, vastuukysymyksiin ja tietoturvaan

---

3 Vuoden 2012 erityiseurobarometrikysely 390 kyberturvallisuudesta.

4 Kyberturvallisuudella tarkoitetaan yleisesti varokeinoja ja toimenpiteitä, joilla voidaan suojata verkkoympäristöä sekä siviili- että sotilaspuolella uhkilta, jotka liittyvät tai voivat haitallisesti vaikuttaa sen muodostaviin keskinäisriippuvaisiin verkkoihin ja tietoinfrastruktuureihin. Kyberturvatoimilla pyritään säilyttämään verkkojen ja infrastruktuurin käytettävyys ja eheys sekä niiden sisältämien tietojen luottamuksellisuus.

5 Verkkorikollisuudella viitataan yleisesti monenlaiseen erityyppiseen rikolliseen toimintaan, jossa tietokoneet ja tietojärjestelmät ovat pääasiallisena välineenä tai pääasiallisena kohteena. Verkkorikollisuus kattaa perinteiset rikokset (kuten petokset, väärennökset ja identiteettivarkaudet), sisältöön liittyvät rikokset (kuten lapsipornografian verkkolevitys tai rotuvihaan kiihottaminen) sekä tietokoneille ja tietojärjestelmille ominaiset rikokset (kuten hyökkäykset tietojärjestelmiä kohtaan, palvelunestohyökkäykset ja haittaohjelmat).

liittyvien vaatimusten tarve on käymässä yhä ilmeisemmäksi. Tässä strategiassa selvennetään periaatteita, joiden tulisi ohjata kyberturvallisuuspolitiikkaa EU:ssa ja kansainvälisesti.

EU:n ydinarvot pätevät yhtä hyvin digitaalisessa kuin fyysisessäkin maailmassa

Samat lait ja normit, jotka säätelevät päivittäin elämämme muita osa-alueita, koskevat myös verkkoympäristöä.

Perusoikeuksien, ilmaisunvapauden, henkilötietojen ja yksityisyyden suojaaminen

Kyberturvallisuus voi olla vakaalla pohjalla ja tuloksellista vain jos se perustuu Euroopan unionin perusoikeuskirjassa vahvistettuihin perusoikeuksiin ja -vapauksiin ja EU:n ydinarvoihin. Vastaavasti yksityishenkilöiden oikeuksia ei voida varmistaa ilman turvallisia verkkoja ja järjestelmiä. Kaikessa kyberturvallisuustarkoituksiin suoritettavassa tietojenvaihdossa, kun on kyse henkilötiedoista, olisi noudatettava EU:n tietosuojalainsäädäntöä ja otettava täysimääräisesti huomioon yksityishenkilöiden oikeudet tällä alalla.

Pääsy kaikille

Rajoitettu pääsy internetiin tai sen puuttuminen kokonaan ja digitaalinen lukutaidottomuus asettavat kansalaiset eriarvoiseen asemaan, kun otetaan huomioon, miten laajasti digitaalimaailma on tullut osaksi yhteiskunnan toimintoja. Jokaisella tulisi olla mahdollisuus internetin käyttöön ja rajoittamattomaan tiedonkulkuun. Internetin eheys ja tietoturva on taattava, jotta kaikilla olisi turvallinen mahdollisuus hyötyä siitä.

Demokraattinen ja tehokas monen toimijan hallinto

Digitaalimaailma ei ole yksittäisen tahon valvonnassa. Tällä hetkellä internetin resurssien, yhteyskäytäntöjen ja standardien päivittäiseen hallinnointiin ja internetin jatkokehitykseen osallistuu useita toimijoita, joista monet ovat kaupallisia ja valtiosta riippumattomia. EU tunnustaa edelleen kaikkien nykyiseen internetin hallintomalliin kuuluvien sidosryhmien merkityksen ja tukee tällaista monen toimijan hallintotapaa[6].

Yhteinen vastuu tietoturvan varmistamisesta

Kasvava riippuvuus tieto- ja viestintäteknologiasta kaikilla ihmiselämän osa-alueilla on tuonut mukanaan haavoittuvuuksia, jotka on määriteltävä asianmukaisesti, analysoitava perusteellisesti ja korjattava tai rajattava pienemmiksi. Kaikkien asiaan kuuluvien toimijoiden, niin viranomaisten ja yksityisen sektorin kuin yksittäisten kansalaistenkin on tunnustettava tämä yhteinen vastuu, ryhdyttävä toimiin itsensä suojaamiseksi ja tarvittaessa varmistettava koordinoitu toiminta kyberturvallisuuden lujittamiseksi.

2. STRATEGISET PAINOPISTEET JA TOIMET

EU:n olisi turvattava verkkoympäristö, joka tarjoaa mahdollisimman laajan vapauden ja tietoturvan kaikkien hyödyksi. Vaikka verkkoympäristön turvallisuushaasteet kuuluvatkin pääasiallisesti jäsenvaltioille, tässä strategiassa ehdotetaan erityistoimia, joilla voidaan parantaa EU:n kokonaissuoriutumista asiassa. Toimenpiteisiin kuuluu sekä lyhyen että pitkän

[6] Ks. myös KOM(2009) 277: *Komission tiedonanto Euroopan parlamentille ja neuvostolle - Internetin hallinto tästä eteenpäin.*

aikavälin toimia ja erilaisia politiikan välineitä[7], ja niissä on mukana eri tyyppisiä toimijoita EU:n toimielimistä jäsenvaltioihin ja yritysmaailmaan.

Tässä strategiassa esitelty EU:n visio rakentuu viidelle strategiselle painopisteelle, jotka liittyvät edellä kuvailtuihin haasteisiin:

- Verkon vakaus
- Verkkorikollisuuden huomattava vähentäminen
- Yhteiseen turvallisuus- ja puolustuspolitiikkaan (YTPP) liittyvän verkkopuolustuspolitiikan ja valmiuksien kehittäminen
- Kyberturvallisuuteen liittyvien teollisten ja teknologisten voimavarojen kehittäminen
- Johdonmukaisen kansainvälisen verkkotoimintapolitiikan luominen Euroopan unionille sekä EU keskeisten arvojen edistäminen

2.1. Verkon vakaus

Verkon vakauden edistäminen EU:ssa edellyttää, että sekä viranomaiset että yksityinen sektori parantavat valmiuksiaan ja tekevät tuloksellista yhteistyötä. Toistaiseksi toteutetuissa toimissa[8] saavutettuja myönteisiä tuloksia hyödyntämällä ja toteuttamalla tarvittavia EU:n lisätoimia voidaan erityisesti auttaa lieventämään verkkoriskejä ja uhkia, joilla on rajat ylittävä ulottuvuus, sekä edesauttaa koordinoitua toimintaa hätätilanteissa. Näin tuettaisiin merkittävästi sisämarkkinoiden toimintaa ja parannettaisiin EU:n sisäistä turvallisuutta.

Eurooppa pysyy haavoittuvana, ellei ryhdytä toden teolla parantamaan julkisia ja yksityisiä valmiuksia, resursseja ja prosesseja kyberturvallisuuspoikkeaminen ehkäisemiseksi, havaitsemiseksi ja käsittelemiseksi. Tästä syystä komissio on laatinut erityisen verkko- ja tietoturvapolitiikan[9]. **Euroopan verkko- ja tietoturvavirasto ENISA** perustettiin vuonna 2004[10] ja neuvostossa ja parlamentissa käsitellään parhaillaan uutta asetusta ENISAn vahvistamisesta ja sen toimeksiannon nykyaikaistamisesta[11]. Lisäksi sähköisen viestinnän puitedirektiivissä edellytetään[12], että sähköisten viestintäpalvelujen tarjoajat hallitsevat asianmukaisesti verkkoihinsa kohdistuvia riskejä ja raportoivat merkittävistä turvallisuuspoikkeamista. EU:n tietosuojalainsäädännön[13] mukaan rekisterinpitäjien on varmistettava tietosuojavaatimusten noudattaminen ja varotoimenpiteiden käyttö, ja myös tarvittavat turvatoimenpiteet. Yleisesti saatavilla olevien sähköisen viestinnän palvelujen tapauksessa rekisterinpitäjien on ilmoitettava toimivaltaisille kansallisille viranomaisille turvallisuuspoikkeamista, joissa on kyse henkilötietosuojaloukkauksista.

---

7 Kaikessa tietojenvaihdossa, kun on kyse henkilötiedoista, olisi noudatettava EU:n tietosuojalainsäädäntöä.

8 Ks. viittaukset tässä tiedonannossa sekä vaikutustenarvioinnissa, joka liittyy komission ehdotukseen direktiiviksi verkko- ja tietoturvasta, ja erityisesti sen kohdissa 4.1.4 ja 5.2 sekä liitteissä 2, 6 ja 8.

9 Vuonna 2001 komissio antoi tiedonannon *Verkko- ja tietoturva: Ehdotus eurooppalaiseksi lähestymistavaksi* (KOM(2001) 298); vuonna 2006 se hyväksyi *Turvallisen tietoyhteiskunnan strategian* (KOM(2006) 251). Vuoden 2009 jälkeen komissio on myös hyväksynyt toimintasuunnitelman ja tiedonannon elintärkeiden tietoinfrastruktuureiden suojaamisesta (KOM(2009) 149), jonka neuvosto hyväksyi päätöslauselmassaan 2009/C 321/01, sekä KOM(2011) 163, jonka neuvosto hyväksyi päätelmissään 10299/11.

10 Asetus (EY) N:o 460/2004.

11 KOM(2010) 521. Tässä strategiassa ehdotetut toimet eivät edellytä muutoksia ENISAn nykyiseen tai tulevaan toimeksiantoon.

12 Direktiivin 2002/21/EY 13 a ja 13 b artikla.

13 Direktiivin 95/46/EY 17 artikla; direktiivin 2002/58/EY 4 artikla.

Vaikka vapaaehtoisten sitoumusten pohjalta onkin saavutettu edistystä, eri puolilla EU:ta on edelleen puutteita kansallisissa valmiuksissa, koordinoinnissa rajat ylittävissä turvallisuuspoikkeamissa ja yksityisen sektorin osallistumisessa ja valmiusasteessa. Tämän strategian ohella annetaan **lainsäädäntöehdotus**, jolla pyritään erityisesti:

- vahvistamaan kansallisen tason verkko- ja tietoturvalle yhteiset minimivaatimukset, joilla velvoitettaisiin jäsenvaltiot: nimeämään verkko- ja tietoturvasta vastaavat kansalliset toimivaltaiset viranomaiset, perustamaan toimiva CERT-ryhmä ja hyväksymään kansallinen verkko- ja tietoturvastrategia ja kansallinen verkko- ja tietoturvan yhteistyösuunnitelma; kapasiteetin lisääminen ja koordinointi koskevat myös EU:n toimielimiä: vuonna 2012 perustettiin pysyvästi EU:n toimielinten, virastojen ja elinten tietotekniikkajärjestelmien tietoturvasta vastaava CERT-EU-ryhmä,
- luomaan koordinoituja ehkäisy-, havaitsemis-, lieventämis- ja reagointimekanismeja, jotka mahdollistavat tietojenvaihdon ja keskinäisen avunannon verkko- ja tietoturvan alalla toimivaltaisten kansallisten viranomaisten kesken; verkko- ja tietoturva-alan toimivaltaisten kansallisten viranomaisten tehtävänä on varmistaa erityisesti EU-tason verkko- ja tietoturvayhteistyösuunnitelman pohjalta tarvittava EU:n laajuinen yhteistyö, jonka tarkoituksena on vastata kyberturvallisuuspoikkeamiin, joilla on rajat ylittäviä ulottuvuuksia; tässä yhteistyössä hyödynnetään myös Euroopan jäsenvaltiofoorumin (EFMS)[14] tuloksia; foorumissa on käyty hedelmällisiä keskusteluja ja ajatustenvaihtoa verkko- ja tietoturvapolitiikasta ja se voidaan liittää luotavaan yhteistyömekanismiin,
- parantamaan yksityisen sektorin valmiusastetta ja osallistumista; koska suuri enemmistö verkko- ja tietojärjestelmistä on yksityisessä omistuksessa ja käytössä, yksityisen sektorin osallisuuden parantaminen on keskeisen tärkeää kyberturvallisuuden edistämiseksi; yksityisen sektorin olisi kehitettävä teknisellä tasolla omia verkon vakauden ylläpitovalmiuksiaan ja jaettava tietoa parhaista käytänteistä eri alojen välillä; alalla kehitetyistä välineistä, joilla turvallisuuspoikkeamiin vastataan, selvitetään niiden syitä ja tutkitaan niiden taustoja, olisi päästävä hyötymään myös julkisella sektorilla.

Yksityisillä toimijoilla ei kuitenkaan edelleenkään ole todellisia kannustimia antaa luotettavaa tietoa verkko- ja tietoturvapoikkeamista ja niiden vaikutuksista, omaksua asianmukainen riskienhallintakulttuuri tai investoida tietoturvaratkaisuihin. Ehdotetulla lainsäädännöllä pyritäänkin varmistamaan, että tiettyjen keskeisten alojen (energia, liikenne, pankkitoiminta, arvopaperipörssit ja keskeisten internet-palvelujen mahdollistajat sekä julkishallinnot) toimijat arvioivat kyberturvallisuusriskinsä, varmistavat verkkojen ja tietojärjestelmien luotettavuuden ja vakauden asianmukaisella riskinhallinnalla sekä jakavat hankkimansa tiedon verkko- ja tietoturvasta vastaavien kansallisten toimivaltaisten viranomaisten kanssa. Kyberturvallisuuskulttuurin omaksuminen voisi parantaa liiketoimintamahdollisuuksia ja kilpailukykyä yksityisellä sektorilla, ja kyberturvallisuudesta voisi tulla myyntivaltti.

Kyseisten tahojen olisi raportoitava toimivaltaisille kansallisille verkko- ja tietoturvaviranomaisille poikkeamista, joilla on merkittäviä vaikutuksia verkko- ja tietojärjestelmiin tukeutuvien keskeisten palvelujen ja tavarantoimitusten jatkuvuuteen.

Kansallisten toimivaltaisten verkko- ja tietoturvaviranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoa muiden sääntelyelinten ja erityisesti tietosuojaviranomaisten kanssa. Toimivaltaisten verkko- ja tietoturvaviranomaisten olisi raportoiva poikkeamista, joihin

[14] Euroopan jäsenvaltiofoorumi perustettiin tiedonannolla KOM(2009) 149. Se tarjoaa puitteet jäsenvaltioiden viranomaisten keskusteluille hyvistä toimintakäytänteistä kriittisten tietoinfrastruktuurien suojaamisen ja sietokyvyn alalla.

epäillään liittyvän vakavaa rikollisuutta, lainvalvontaviranomaisille. Kansallisten toimivaltaisten viranomaisten olisi säännöllisesti julkaistava erillisellä verkkosivustolla ei-luottamukselliset tiedot voimassa olevista poikkeama- ja riskivaroituksista ja koordinoiduista reagointitavoista. Oikeudellisten velvoitteiden ei pitäisi korvata eikä ehkäistä epävirallista ja vapaaehtoista yhteistyötä muun muassa julkisen ja yksityisen sektorin välillä turvallisuustasojen korottamiseksi ja tietojen vaihtamiseksi ja parhaiden käytäntöjen levittämiseksi. Varsinkin järjestelmien sietokyvyn parantamiseen tähtäävä eurooppalainen julkis-yksityinen kumppanuus (EP3R[15]) on toimiva ja hyödyllinen EU-tason foorumi, jota olisikin edelleen kehitettävä.

Verkkojen Eurooppa -välineestä (CEF)[16] voitaisiin saada rahoitustukea keskeisille infrastruktuureille, joilla liitettäisiin yhteen jäsenvaltioiden verkko- ja tietoturvavalmiudet ja helpotettaisiin näin yhteistyötä koko EU:ssa.

EU-tasoiset kyberturvallisuusharjoitukset ovat olennainen tekijä simuloitaessa yhteistyötä jäsenvaltioiden ja yksityisen sektorin kesken. Ensimmäinen jäsenvaltioiden harjoitus (*Cyber Europe 2010*) järjestettiin vuonna 2010 ja toinen, jossa oli mukana myös yksityinen sektori, lokakuussa 2012 (*Cyber Europe 2012*). Marraskuussa 2011 pidettiin EU:n ja Yhdysvaltojen yhteinen simulaatioharjoitus (*Cyber Atlantic 2011*). Lähivuosille on suunnitteilla lisää harjoituksia, myös kansainvälisten kumppanien kanssa.

Komissio

- jatkaa Yhteisen tutkimuskeskuksen JRC:n kautta ja koordinoidusti jäsenvaltioiden viranomaisten ja kriittisten infrastruktuurien omistajien ja ylläpitäjien kanssa toimia, joilla pyritään tunnistamaan Euroopan kriittisten infrastruktuurien verkko- ja tietoturvaan liittyvät haavoittuvuudet ja edistämään vakaiden järjestelmien kehitystä,
- käynnistää vuoden 2013 alkupuolella EU-rahoitteisen pilottihankkeen[17], joka koskee **bottiverkkojen ja haittaohjelmistojen torjuntaa** ja muodostaa puitteet EU:n jäsenvaltioiden, yksityisen sektorin toimijoiden, kuten internet-palveluntarjoajien, ja kansainvälisten kumppanien koordinoinnille ja yhteistyölle.

Komissio pyytää ENISAa

- avustamaan jäsenvaltioita vahvojen **kansallisten kybersuojautumisvalmiuksien** kehittämisessä erityisesti rakentamalla osaamista teollisuuden toiminnanohjausjärjestelmien sekä liikenne- ja energiainfrastruktuurin turvaamisen ja sietokyvyn alalla,
- selvittämään vuoden 2013 aikana mahdollisuuksia perustaa EU:hun teollisuuden toiminnanohjausjärjestelmiin keskittyneitä ICS-CSIRT-ryhmiä (*Computer Security Incident Response Team for Industrial Control Systems*),

15 Kumppanuus käynnistettiin tiedonannon KOM(2009) 149 pohjalta. Foorumi käynnistänyt toimet ja edistänyt yhteistyötä julkisen ja yksityisen sektorin välillä pyrkimyksenään yksilöidä keskeiset hyödykkeet, resurssit, toiminnot ja sietokyvyn perusvaatimukset sekä yhteistyötarpeet ja mekanismit, joilla voidaan vastata sähköiseen viestintään vaikuttaviin suuren mittakaavan häiriöihin.

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. Budjettikohta 09.03.02 – Televiestintäverkot (kansallisten julkisten palvelujen verkkoon liittäminen ja yhteentoimivuus sekä pääsy tällaisiin verkkoihin).

17 CIP-ICT PSP-2012-6, 325188. Kokonaisbudjetti 15 miljoonaa euroa, EU:n rahoitusosuus 7,7 miljoonaa euroa.

- jatkamaan jäsenvaltioiden ja EU-toimielinten tukemista järjestettäessä säännöllisiä **yleiseurooppalaisia kyberturvallisuusharjoituksia**, jotka muodostavat myös operatiivisesti perustan EU:n osallistumiselle kansainvälisiin kyberturvallisuusharjoituksiin.

Komissio pyytää Euroopan parlamenttia ja neuvostoa

- **hyväksymään** viivytyksittä **verkko- ja tietoturvan yhteisen korkean tason** varmistamista unionissa käsittelevän direktiiviehdotuksen, joka koskee kansallisia valmiuksia ja varautumistasoa, EU-tason yhteistyötä, riskinhallintakäytänteiden käyttöönottoa ja verkko- ja tietoturvaan liittyvää tiedonvaihtoa.

Komissio pyytää teollisuutta

- ottamaan vetovastuun korkeatasoiseen kyberturvallisuuteen **investoimisessa** ja parhaiden käytänteiden ja tiedonvaihdon kehittämisessä toimialatasolla ja viranomaisten kanssa tavoitteena varmistaa tuotantohyödykkeiden ja yksityishenkilöiden vahva ja tuloksellinen suojaaminen erityisesti EP3R- ja TDL (*Trust in Digital Life*)[18] -hankkeiden kaltaisten julkisen ja yksityisen sektorin kumppanuuksien kautta.

Valveuttaminen

Kyberturvallisuuden varmistaminen on yhteisellä vastuullamme. Loppukäyttäjät ovat keskeisessä asemassa varmistettaessa verkkojen ja tietojärjestelmien turvallisuutta: heidät on saatava tietoisiksi verkon riskeistä ja suorittamaan yksinkertaisia toimenpiteitä riskeiltä suojautumiseksi.

Alalla on viime vuosina käynnistetty useita hankkeita, joita olisi jatkettava. ENISA on osallistunut valveuttamiseen julkaisemalla raportteja, järjestämällä asiantuntijaseminaareja ja kehittämällä julkisen ja yksityisen sektorin kumppanuuksia. Myös Europol, Eurojust ja kansalliset tietosuojaviranomaiset ovat aktiivisesti mukana valveuttamistoiminnassa. Lokakuussa 2012 ENISA pilotoi joidenkin jäsenvaltioiden kanssa kyberturvallisuuden teemakuukautta (*European Cybersecurity Month*). Valveuttaminen on yksi EU:n ja Yhdysvaltojen kyberturvallisuus- ja verkkorikollisuustyöryhmän[19] toiminta-aloista ja keskeisellä sijalla myös *Safer Internet* -ohjelmassa[20] (jossa keskitytään lasten turvalliseen verkonkäyttöön).

Komissio pyytää ENISAa

- ehdottamaan vuonna 2013 suunnitelmaa "verkko- ja tietoturva-ajokortin" luomiseksi tavoitteena perustaa vapaaehtoisuuteen perustuva sertifiointiohjelma edistämään tarvittavaa osaamista ja pätevyyttä tietotekniikan ammattilaisten

[18] http://www.trustindigitallife.eu/.

[19] EU:n ja Yhdysvaltojen huippukokouksessa marraskuussa 2010 (MEMO/10/597) perustetun työryhmän tehtävänä on kehittää yhteistyömahdollisuuksia monenlaisissa kyberturvallisuuteen ja verkkorikollisuuteen liittyvissä kysymyksissä.

[20] *Safer Internet* -ohjelmassa rahoitetaan järjestöistä koostuvaa verkostoa, joka toimii lasten verkonkäytön turvallisuuden alalla, lainkäyttöelinten verkostoa, jossa vaihdetaan tietoa ja parhaita käytänteitä lasten seksuaaliseen hyväksikäyttöön liittyvän materiaalin verkkolevityksen torjunnassa sekä tutkijaverkostoa, joka kokoaa tietoa verkkoteknologioiden käytöstä, riskeistä ja vaikutuksista lasten näkökulmasta.

(esim. verkkosivustojen ylläpitäjien) keskuudessa.

Komissio

- järjestää yhdessä ENISAn kanssa vuonna 2014 **kyberturvallisuuskilpailun**, jossa yliopisto-opiskelijat kilpailevat verkko- ja tietoturvaa koskevilla ratkaisuehdotuksillaan.

Komissio pyytää jäsenvaltioita[21]

- järjestämään vuodesta 2013 lähtien ENISAn tuella ja yksityisen sektorin kanssa **kyberturvallisuuskuukauden**, jonka tarkoituksena on lisätä asiaa koskevaa tietoisuutta loppukäyttäjien keskuudessa; EU:n ja Yhdysvaltain samanaikaista kyberturvallisuuskuukautta aletaan viettää vuodesta 2014 lähtien,
- **tehostamaan kansallisia toimia verkko- ja tietoturvaopetuksen ja -koulutuksen alalla** aloittamalla kouluissa verkko- ja tietoturvaopetus vuoteen 2014 mennessä, antamalla tietotekniikan opiskelijoille opetusta verkko- ja tietoturvasta, tietoturvallisten ohjelmistojen kehittämisestä ja henkilötietojen suojasta sekä antamalla julkishallinnon työntekijöille peruskoulutusta verkko- ja tietoturvan alalla.

Komissio pyytää teollisuutta

- edistämään kyberturvallisuutta koskevaa **tietoisuutta kaikilla tasoilla** niin liiketoimintakäytänteissä kuin asiakasrajapinnallakin; teollisuuden olisi erityisesti pohdittava tapoja lisätä toimitusjohtajien ja hallitusjäsenten vastuuta kyberturvallisuuden varmistamisesta.

2.2. Verkkorikollisuuden huomattava vähentäminen

Mitä digitaalisemmassa maailmassa elämme, sitä suuremmat ovat verkkorikollisille avautuvat mahdollisuudet. Verkkorikollisuus on yksi nopeimmin lisääntyvistä rikollisuuden muodoista: sen uhriksi joutuu maailmassa yli miljoona ihmistä joka päivä. Verkkorikollisista ja verkkorikollisverkostoista on tullut entistä kehittyneempiä, ja tarvitsemmekin asiaan puuttumiseksi oikeat operatiiviset välineet ja valmiudet. Verkkorikokset tarjoavat mahdollisuuden suuriin voittoihin pienellä riskillä ja rikolliset hyödyntävät usein anonyymejä verkkotunnusalueita. Verkkorikollisuus ei tunnusta kansallisia rajoja. Internetin globaalin luonteen vuoksi lainvalvontaviranomaisten on omaksuttava koordinoitu ja rajat ylittävän yhteistyön mahdollistava lähestymistapa vastatakseen tähän kasvavaan uhkaan.

Vahva ja toimiva lainsäädäntö

EU ja sen jäsenvaltiot tarvitsevat vahvaa ja tuloksellista lainsäädäntöä verkkorikollisuutta vastaan. Tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus (ns. Budapestin sopimus) on sitova kansainvälinen sopimus, joka muodostaa toimivat puitteet kansalliselle lainsäädännölle.

EU on jo antanut tietoverkkorikollisuuteen liittyvää lainsäädäntöä, josta esimerkkinä direktiivi lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian

[21] Niin, että mukana ovat myös asiaan liittyvät kansalliset viranomaiset, kuten toimivaltaiset verkko- ja tietoturvaviranomaiset ja tietosuojaviranomaiset.

torjumisesta[22]. EU on myös hyväksymässä direktiivin erityisesti bottiverkkojen avulla tehtävistä tietoverkkohyökkäyksistä.

Komissio

- varmistaa verkkorikollisuuteen liittyvien direktiivien viivästymättömän täytäntöönpanon,
- kehottaa niitä jäsenvaltioita, jotka eivät vielä ole ratifioineet **tietoverkkorikollisuutta koskevaa Euroopan neuvoston yleissopimusta (Budapestin sopimusta)**, ratifioimaan ja täytäntöönpanemaan sen määräykset mahdollisimman nopeasti.

Paremmat operatiiviset valmiudet verkkorikollisuuden torjuntaan

Verkkorikoksissa käytettyjen tekniikoiden kehitys on nopeutunut huimaa vauhtia: lainvalvontaviranomaiset eivät voi taistella verkkorikollisuutta vastaan vanhentuneilla välineillä. Kaikilla EU:n jäsenvaltioilla ei tällä hetkellä ole verkkorikollisuuden torjunnan edellyttämiä operatiivisia valmiuksia. Kaikki jäsenvaltiot tarvitsevat tuloksellisen kansallisen verkkorikosyksikön.

Komissio

- tukee rahoitusohjelmiensa kautta[23] jäsenvaltioita niiden pyrkiessä **tunnistamaan puutteet ja vahvistamaan valmiuksiaan** tutkia ja torjua verkkorikollisuutta; lisäksi komissio tukee tahoja, jotka luovat yhteyksiä tutkimuslaitosten, lainkäyttöviranomaisten ja yksityisen sektorin välillä vastaavalla tavalla kuin parhaillaan tehdään joihinkin jäsenvaltioihin jo perustetuissa komission rahoittamissa verkkorikollisuuden torjunnan osaamiskeskittymissä,
- koordinoi yhdessä jäsenvaltioiden kanssa ja muun muassa JRC:n tuella pyrkimyksiä löytää parhaat käytänteet ja parhaat käytettävissä olevat tekniikat verkkorikollisuuden torjumiseksi (esim. rikostutkinnallisten välineiden kehittämisen ja käytön tai uhka-analyysien alalla),
- tekee tiivistä yhteistyötä hiljattain perustetun **Euroopan verkkorikostorjuntakeskuksen (EC3), Europolin ja Eurojustin** kanssa toimintapolitiikan yhdenmukaistamiseksi operatiivisen puolen parhaiden käytäntöjen kanssa.

Parempi EU-tason koordinointi

EU voi täydentää jäsenvaltioiden työtä tukemalla koordinoitua ja yhteistyöhön perustuvaa lähestymistapaa, joka kokoaa yhteen lainvalvonta- ja oikeusviranomaiset sekä julkiset ja yksityiset sidosryhmät EU:sta ja laajemminkin.

[22] Direktiivi 2011/93/EU neuvoston puitepäätöksen 2004/68/YOS korvaamisesta.

[23] Vuonna 2013 rikosten ennalta ehkäisyä ja torjuntaa koskevasta erityisohjelmasta (ISEC). Vuoden 2013 jälkeen sisäisen turvallisuuden rahastosta (monivuotiseen rahoituskehykseen sisältyvä uusi rahoitusväline).

Komissio

- tukee hiljattain perustettua **Euroopan verkkorikostorjuntakeskusta** (EC3), joka toimii verkkorikollisuuden torjunnan keskipisteenä Euroopassa; EC3 tuottaa analyysejä ja tiedustelutietoa, tukee rikostutkintaa, tarjoaa korkean tason tutkinnallista apua, helpottaa yhteistyötä, luo tiedonvaihtokanavia jäsenvaltioiden toimivaltaisten viranomaisten, yksityisen sektorin ja muiden sidosryhmien välille sekä tulee asteittain toimimaan lainvalvontayhteisön yhteisenä äänenä[24],
- tukee pyrkimyksiä lisätä unionin lainsäädännön, myös tietosuojasääntöjen, mukaisesti verkkotunnusten rekisterinpitäjien vastuuta ja varmistaa verkkosivustojen omistustietojen oikeellisuus käyttäen perustana ICANNille (*Internet Corporation for Assigned Names and Numbers*) annettuja lainvalvontaa koskevia suosituksia,
- lujittaa hiljattain annetun lainsäädännön pohjalta edelleen EU:n pyrkimyksiä puuttua verkossa tapahtuvaan lasten seksuaaliseen hyväksikäyttöön; komissio on hyväksynyt eurooppalaisen strategian internetin parantamiseksi lasten näkökulmasta[25] ja käynnistänyt yhdessä EU-maiden ja EU:n ulkopuolisten maiden kanssa **maailmanlaajuisen kumppanuuden verkossa esiintyvän lasten seksuaalisen hyväksikäytön torjumiseksi[26]**; kumppanuus toimii välineenä lisätoimille, joita jäsenvaltiot toteuttavat komission ja EC3:n tuella.

Komissio pyytää Europolia (EC3)

- aluksi keskittämään analyyttisen ja operatiivisen tukensa jäsenvaltioiden verkkorikostutkintayksiköille auttaakseen purkamaan verkkorikollisverkostoja ja estämään niiden toimintaa ensisijaisesti lasten seksuaalisen hyväksikäytön, maksupetosten, bottiverkkojen ja tietoverkkoihin tunkeutumisen alalla,
- laatimaan säännöllisesti strategisia ja operatiivisia raportteja kehityssuuntauksista ja esiin nousevista uhkista painopisteiden määrittelemiseksi ja jäsenvaltioiden verkkorikollisuusryhmien tutkintatoiminnan kohdistamiseksi.

Komissio pyytää Euroopan poliisiakatemiaa (CEPOL) yhteistyössä Europolin kanssa

- koordinoimaan koulutuskurssien suunnittelua, jotta lainvalvontaviranomaisille saataisiin annettua tarvittava osaaminen ja ammattitaito puuttua tehokkaasti verkkorikollisuuteen.

Komissio pyytää Eurojustia

- yksilöimään suurimmat esteet oikeusyhteistyölle verkkorikostutkinnassa ja jäsenvaltioiden ja kolmansien maiden väliselle koordinoinnille sekä tukemaan verkkorikosten tutkintaa ja syyteharkintaa sekä operatiivisella että strategisella tasolla, sekä tukemaan alan koulutustoimintaa.

---

24 Euroopan komissio antoi 28. maaliskuuta 2012 tiedonannon *Rikostentorjunta digitaaliaikana: Euroopan verkkorikostorjuntakeskuksen perustaminen*.

25 COM(2012) 196 final.

26 Neuvoston päätelmät maailmanlaajuisesta kumppanuudesta verkossa esiintyvän lasten seksuaalisen hyväksikäytön torjumiseksi (EU:n ja Yhdysvaltojen yhteislausuma), 7.-8. kesäkuuta 2012, sekä julistus maailmanlaajuisen kumppanuuden käynnistämisestä verkossa esiintyvän lasten seksuaalisen hyväksikäytön torjumiseksi (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

Komissio pyytää Eurojustia ja Europolia (EC3)

- tekemään tiivistä yhteistyötä muun muassa tiedonvaihdon kautta, jotta ne pystyisivät tuloksellisemmin torjumaan verkkorikollisuutta toimivaltansa rajoissa.

2.3. Yhteiseen turvallisuus- ja puolustuspolitiikkaan (YTPP) liittyvän verkkopuolustuspolitiikan ja valmiuksien kehittäminen

EU:n kyberturvallisuustavoitteilla on myös kyberpuolustukseen liittyvä ulottuvuus. Jotta jäsenvaltioiden puolustuspoliittisia ja kansalliseen turvallisuuteen liittyviä etuja suojaavien tieto- ja viestintäjärjestelmien sietokykyä voitaisiin parantaa, kyberpuolustusvalmiuksien kehittämisessä olisi keskityttävä sofistikoitujen verkkouhkien havaitsemiseen, niihin vastaamiseen ja niistä toipumiseen.

Koska uhat ovat monitahoisia, olisi hyödynnettävä synergioita kriittisten verkkoresurssien suojaamiseen liittyvien siviili- ja sotilaspuolen ratkaisujen välillä. Näitä pyrkimyksiä olisi tuettava tutkimus- ja kehitystoimin sekä tiiviimmällä yhteistyöllä hallitusten, yksityisen sektorin ja tutkimusyhteisön välillä EU:ssa. Päällekkäisen työn välttämiseksi EU selvittelee, miten EU ja NATO voisivat keskinäisesti täydentää pyrkimyksiään parantaa sellaisten kriittisten valtiollisten, puolustuksellisten ja muiden tietoinfrastruktuurien sietokykyä, joista molemmat ovat riippuvaisia.

Korkea edustaja keskittyy seuraaviin avaintoimiin ja pyytää jäsenvaltioita ja Euroopan puolustusvirastoa (EDA) kanssaan yhteistyöhön:

- arvioidaan EU:n kyberpuolustuksen operatiivisia vaatimuksia ja edistetään EU:n kyberpuolustusvalmiuksien ja -teknologioiden kehitystä valmiuksien lujittamiseksi kaikilla osa-alueilla, joihin lukeutuvat doktriini, johtajuus, organisointi, henkilöstö, koulutus, teknologia, infrastruktuuri, logistiikka ja yhteentoimivuus,

- kehitetään EU:n kyberpuolustuspoliittista kehystä verkkojen suojaamiseksi yhteisen turvallisuus- ja puolustuspolitiikan operaatioiden puitteissa, mukaan luettuina dynaaminen riskienhallinta, paremmat uhka-analyysit ja tiedonvaihto; parannetaan puolustusvoimien mahdollisuuksia kyberpuolustukseen liittyvään koulutukseen ja harjoitteluun eurooppalaisessa ja monikansallisessa kontekstissa; tähän sisältyy myös kyberpuolustusosioiden sisällyttäminen nykyisiin harjoitussuunnitelmiin,

- edistetään siviili- ja sotilastoimijoiden vuoropuhelua ja koordinointia EU:ssa kiinnittäen erityistä huomiota hyvien käytänteiden levittämiseen, tiedonvaihtoon, varhaisvaroitusjärjestelmiin, turvapoikkeamareagointiin, riskiarviointiin, tietoisuuden lisäämiseen ja kyberturvallisuuden prioriteettiaseman vahvistamiseen,

- varmistetaan vuoropuhelu kansainvälisten kumppanien kanssa, mukaan luettuina NATO, muut kansainväliset järjestöt ja monikansalliset osaamiskeskukset, jotta voidaan varmistaa toimivat puolustusvalmiudet, tunnistaa yhteistyötä edellyttävät asiat ja välttyä toiminnan päällekkäisyyksiltä.

2.4. Kyberturvallisuuteen liittyvien teollisten ja teknologisten voimavarojen kehittäminen

Euroopalla on erinomaiset tutkimus- ja kehitysvalmiudet, mutta monet maailman johtavista innovatiivisten tieto- ja viestintäteknisten tuotteiden ja palvelujen tarjoajista tulevat EU:n ulkopuolelta. Vaarana on, että Euroopasta tulee liian riippuvainen paitsi muualla tuotetusta tieto- ja viestintätekniikasta myös sen rajojen ulkopuolella kehitetyistä turvallisuusratkaisuista. On olennaisen tärkeää varmistaa, että kriittisissä palveluissa ja infrastruktuureissa ja yhä enenevässä määrin mobiililaitteissa käytettävät EU:ssa ja kolmansissa maissa tuotetut laitteisto- ja ohjelmistokomponentit ovat luotettavia ja tietoturvallisia ja takaavat henkilötietojen suojan.

Kyberturvallisuustuotteiden sisämarkkinoiden edistäminen

Korkea tietoturvataso voidaan varmistaa vain, jos kaikki arvoketjun toimijat (esim. laitevalmistajat, ohjelmistokehittäjät, tietoyhteiskuntapalvelujen tarjoajat) nostavat tietoturvan prioriteetiksi. Näyttää kuitenkin siltä[27], että monet toimijat näkevät edelleen tietoturvan lähinnä lisätaakkana, ja turvaratkaisujen kysyntä on vähäistä. Euroopassa käytettävien tieto- ja viestintätekniikkatuotteiden koko arvoketjussa on noudatettava asianmukaisia kyberturvallisuusvaatimuksia. Yksityiselle sektorille on luotava kannustimia korkeatasoisen kyberturvallisuuden varmistamiseen. Kyberturvallisuudeltaan korkeatasoiset yritykset voisivat esimerkiksi käyttää kyberturvallisuusmerkintöjä myyntivalttina ja saavuttaa näin kilpailuetua. Ehdotettuun verkko- ja tietoturvadirektiiviin sisältyvät velvoitteet auttaisivat myös merkittävästi parantamaan yritysten kilpailukykyä direktiivin kattamilla aloilla.

Tietoturvaltaan korkeatasoisille tuotteille olisi luotava Euroopan laajuista markkinakysyntää. Tällä tiedonannolla pyritäänkin lisäämään yhteistyötä ja avoimuutta tieto- ja viestintäteknisten tuotteiden tietoturvan alalla. Strategian mukaisesti olisi perustettava erityinen foorumi, joka kokoaisi yhteen asiaan kuuluvat eurooppalaiset julkisen ja yksityisen sektorin toimijat määrittelemään hyviä kyberturvallisuuskäytänteitä koko arvoketjussa ja luomaan suotuisia markkinaolosuhteita turvallisten tieto- ja viestintätekniikkaratkaisujen kehittämiselle ja käyttöönotolle. Ensisijaisesti olisi keskityttävä luomaan kannustimia asianmukaiseen riskinhallintaan ja tietoturvastandardien ja -ratkaisujen käyttöönottoon sekä mahdollisesti perustamaan vapaaehtoisuuteen perustuvia EU:n laajuisia sertifiointijärjestelmiä nykyisten EU:ssa ja kansainvälisesti käytössä olevien järjestelmien pohjalta. Komissio edistää yhdenmukaisia lähestymistapoja jäsenvaltioiden kesken, jotta yritykset eivät joutuisi epäedulliseen asemaan sijaintinsa perusteella.

Komissio tukee myös tietoturvastandardien kehittämistä ja avustaa EU:n laajuisia vapaaehtoisia sertifiointijärjestelmiä pilvipalvelujen alalla ottaen asianmukaisesti huomioon tietosuojatarpeet. Toiminnassa olisi keskityttävä koko toimitusketjun tietoturvaan varsinkin kriittisillä talouden aloilla (teollisuuden toiminnanohjausjärjestelmät, energiahuolto ja liikenneinfrastruktuuri). Tässä olisi käytettävä perustana eurooppalaisissa standardointijärjestöissä (CEN, CENELEC ja ETSI) parhaillaan tehtävää työtä[28], kyberturvallisuuden koordinointiryhmän (CSCG) tuloksia sekä ENISAn, komission ja muiden asiaan liittyvien toimijoiden asiantuntemusta.

---

[27] Ks. komission ehdotukseen direktiiviksi verkko- ja tietoturvasta liittyvä vaikutustenarviointi, kohta 4.1.5.2.

[28] Erityisesti älyverkkostandardi M/490, jonka puitteissa laaditaan ensimmäistä standardijoukkoa älyverkoille ja viitearkkitehtuurille.

Komissio

- käynnistää vuonna 2013 **verkko- ja tietoturvaratkaisuja varten julkisen ja yksityisen sektorin foorumin**, jossa kehitetään kannustimia tietoturvallisten tieto- ja viestintäteknisten ratkaisujen käyttöönottoon ja korkeatasoisten kyberturvallisuusvaatimusten asettamiseen Euroopassa käytetyille tieto- ja viestintätekniikkatuotteille,
- laatii foorumin tulosten perusteella vuonna 2014 ehdotuksen suosituksista, joilla varmistettaisiin kyberturvallisuus tieto- ja viestintätekniikan koko arvoketjussa,
- selvittää, miten suurimmat tieto- ja viestintäteknisten laitteistojen ja ohjelmistojen toimittajat voisivat ilmoittaa toimivaltaisille kansallisille viranomaisille todetuista haavoittuvuuksista, joilla voisi olla merkittäviä tietoturvavaikutuksia.

Komissio pyytää ENISAa

- laatimaan yhteistyössä toimivaltaisten kansallisten viranomaisten, asiaan liittyvien sidosryhmien, kansainvälisten ja eurooppalaisten standardointielinten ja Euroopan komission Yhteisen tutkimuskeskuksen JRC:n kanssa **tekniset ohjeet ja suositukset verkko- ja tietoturva-alan standardien ja hyvien käytänteiden** käyttöönotosta julkisella ja yksityisellä sektorilla.

Komissio pyytää julkisen ja yksityisen sektorin toimijoita

- edistämään teollisuusvetoisten tietoturvastandardien, teknisten normien ja yksityisyyden huomioon ottamista jo suunnitteluvaiheessa sekä **tietoturvastandardien** ja kehittämistä ja käyttöönottoa tieto- ja viestintätekniikan valmistajien ja palveluntarjoajien, kuten pilvipalveluntarjoajien, keskuudessa; uusissa laitteisto- ja ohjelmistosukupolvissa olisi oltava **vahvemmat, sulautetut ja käyttäjäystävälliset tietoturvaominaisuudet**,
- kehittämään teollisuusvetoisia standardeja yritysten kyberturvallisuustasolle ja parantamaan yleisötiedotusta kehittämällä **tietoturvamerkintöjä** tai -leimoja, joiden avulla kuluttajien olisi helpompi tehdä valintoja markkinoilla.

T&k-investointien ja innovaatioiden edistäminen

T&k:lla voidaan tukea vahvaa teollisuuspolitiikkaa, edistää luotettavaa eurooppalaista tieto- ja viestintätekniikka-alaa, antaa lisävauhtia sisämarkkinoille ja vähentää Euroopan riippuvuutta ulkomaisesta teknologiasta. T&k:ssa olisi paikattava tieto- ja viestintätekniikan tietoturvan teknologiset aukot, valmistauduttava seuraavan sukupolven tietoturvahaasteisiin, otettava huomioon käyttäjätarpeiden jatkuva muuttuminen ja otettava käyttöön kaksikäyttöteknologioiden tarjoamat hyödyt. Tutkimuksella olisi myös edelleen tuettava salaustekniikoiden kehitystä. Tätä toimintaa on täydennettävä helpottamalla t&k-tulosten jalostamista kaupallisiksi ratkaisuiksi luomalla tarvittavat kannustimet ja sääntelylliset toimintaedellytykset.

EU:n olisi otettava kaikki hyöty irti tutkimuksen ja innovoinnin Horisontti 2020 -puiteohjelmasta[29], jonka on määrä käynnistyä vuonna 2014. Komission ehdotus sisältää

[29] "Horisontti 2020" on Eurooppa 2020 -strategian "Innovaatiounioni"-lippulaivahankkeen täytäntöönpanon rahoitusväline; innovaatiounionin tavoitteena on turvata EU:n globaali kilpailukyky.

luotettavaan tieto- ja viestintätekniikkaan sekä verkkorikollisuuden torjuntaan liittyviä erityistavoitteita, jotka ovat linjassa tämän strategian kanssa. Horisontti 2020 -ohjelmassa tuetaan uusiin tieto- ja viestintäteknologioihin liittyvää tietoturvatutkimusta, kehitetään ratkaisuja koko käyttöketjultaan tietoturvallisia tieto- ja viestintätekniikkajärjestelmiä, -palveluja ja -sovelluksia varten, luodaan kannustimia jo olemassa olevien ratkaisujen käyttöön ja omaksumiseen sekä parannetaan verkko- ja tietojärjestelmien yhteentoimivuutta. EU-tasolla kiinnitetään erityishuomiota eri rahoitusohjelmien (Horisontti 2020, sisäisen turvallisuuden rahasto sekä Euroopan puolustusviraston teettämä tutkimus, mukaan luettuina turvallisuus- ja puolustustutkimuksen eurooppalaiset yhteistyöpuitteet) optimointiin ja parempaan koordinointiin.

Komissio

- kehittää Horisontti 2020 -ohjelman kautta useita tieto- ja viestintätekniikan yksityisyyden suojan ja tietoturvan osa-alueita t&k:sta innovointiin ja käyttöönottoon; Horisontti 2020 -ohjelmassa kehitetään myös työkaluja ja välineitä verkkoympäristöön kohdistuvan rikollisen ja terroristitoiminnan torjumiseksi,
- luo mekanismeja Euroopan unionin toimielinten ja jäsenvaltioiden tutkimuslinjausten parempaa koordinointia varten sekä jäsenvaltioiden kannustamiseksi investoimaan enemmän t&k:hon.

Komissio pyytää jäsenvaltioita

- määrittelemään vuoden 2013 loppuun mennessä hyviä käytänteitä, jotka liittyvät **julkishallintojen ostovoiman** hyödyntämiseen (esimerkiksi julkisten hankintojen kautta) edistettäessä tieto- ja viestintäteknisten tuotteiden ja palvelujen tietoturvaominaisuuksien kehittämistä ja käyttöönottoa,
- edistämään teollisuuden ja tutkimusyhteisön osallistumista varhaisessa vaiheessa ratkaisujen kehittämiseen ja koordinointiin; tässä olisi hyödynnettävä mahdollisimman hyvin Euroopan teollista perustaa ja siihen liittyvällä t&k:lla aikaansaatavia teknologiainnovaatioita ja koordinoitava toimintaa siviili- ja puolustusorganisaatioiden tutkimusohjelmien välillä.

Komissio pyytää Europolia ja ENISAa

- määrittelemään nähtävillä olevat kehityssuuntaukset ja tarpeet, jotka liittyvät uusiin verkkorikollisuuden ja kyberturvallisuuden ilmiöihin, jotta voidaan kehittää tarvittavia digitaalisen tutkinnan välineitä ja teknologioita.

Komissio pyytää julkisen ja yksityisen sektorin toimijoita

- kehittämään yhteistyössä vakuutusalan kanssa **yhdenmukaisia menetelmiä riskipreemioiden laskentaan**, jolloin tietoturvaan investoineet yritykset voisivat hyötyä alhaisemmista riskipreemioista.

Vuodet 2014–2020 kattava EU:n tutkimuksen ja innovoinnin puiteohjelma on osa pyrkimyksiä luoda uutta kasvua ja uusia työpaikkoja Eurooppaan.

2.5. Johdonmukaisen kansainvälisen verkkotoimintapolitiikan luominen Euroopan unionille sekä EU:n keskeisten arvojen edistäminen

Verkon pitäminen avoimena, vapaana ja turvallisena on maailmanlaajuinen haaste, johon EU:n olisi vastattava yhdessä kansainvälisten kumppanien ja organisaatioiden, yksityisen sektorin ja kansalaisyhteiskunnan kanssa.

Kansainvälisessä verkkotoimintapolitiikassa EU pyrkii edistämään internetin avoimuutta ja vapautta, kannustamaan pyrkimyksiä luoda toimintanormeja ja soveltaa verkkoa koskevaa voimassa olevaa kansainvälistä oikeutta. EU pyrkii myös poistamaan digitaalisen kahtiajaon ja osallistuu aktiivisesti kansainvälisiin pyrkimyksiin parantaa kyberturvallisuusvalmiuksia. EU:n kansainvälistä toimintaa verkkoon liittyvissä asioissa ohjaavat EU:n perusarvot: ihmisarvon kunnioittaminen, vapaus, demokratia, tasa-arvo, oikeusvaltioperiaate ja perusoikeuksien kunnioittaminen.

Verkkoon liittyvien kysymysten huomioon ottaminen EU:n ulkosuhteissa ja yhteisessä ulko- ja turvallisuuspolitiikassa

Komission, korkean edustajan ja jäsenvaltioiden olisi määriteltävä EU:lle johdonmukainen kansainvälinen verkkotoimintapolitiikka, jolla pyrittäisiin lisäämään vuoropuhelua ja vahvistamaan suhteita keskeisten kansainvälisten kumppanien ja organisaatioiden sekä kansalaisyhteiskunnan ja yksityisen sektorin kanssa. EU:n yhteydenpito kansainvälisten kumppanien kanssa verkkokysymyksissä olisi suunniteltava, koordinoitava ja toteutettava siten, että se tuottaa lisäarvoa suhteessa jo olemassa olevaan kahdenväliseen vuoropuheluun EU:n jäsenvaltioiden ja kolmansien maiden välillä. EU antaa entistä enemmän painoarvoa vuoropuhelulle kolmansien maiden kanssa ja keskittyy erityisesti samanhenkisiin kumppaneihin, jotka jakavat EU:n arvot. Se pyrkii korkeatasoiseen tietosuojaan muun muassa tilanteissa, joissa henkilötietoja siirretään kolmansiin maihin. Verkon globaaleihin haasteisiin vastaamiseksi EU pyrkii tiiviimpään yhteistyöhön tällä alalla toimivien organisaatioiden kanssa. Tällaisia ovat esimerkiksi Euroopan neuvosto, OECD, YK, ETYJ, NATO, Afrikan unioni, Kaakkois-Aasian maiden liitto ASEAN ja Amerikan valtioiden järjestö OAS. Kahdenvälisellä tasolla erityisen tärkeää on yhteistyö Yhdysvaltojen kanssa. Sitä kehitetäänkin edelleen varsinkin EU:n ja Yhdysvaltojen välisen kyberturvallisuus- ja verkkorikollisuustyöryhmän puitteissa.

Yksi EU:n kansainvälisen verkkopolitiikan keskeisistä elementeistä on verkkoympäristön vapauden ja perusoikeuksien edistäminen. Internetin saatavuuden laajentaminen todennäköisesti edistää demokraattisia uudistuksia ja niiden leviämistä maailmalla. Lisääntyvä globaali verkottuminen ei saisi tuoda mukanaan sensuuria tai joukkovalvontaa. EU:n olisi edistettävä yritysten yhteiskuntavastuuta[30] ja tehtävä kansainvälisiä aloitteita tämän alan maailmanlaajuisen koordinoinnin parantamiseksi.

Vastuu turvallisemmasta verkosta kuuluu kaikille globaalin tietoyhteiskunnan toimijoille kansalaisista hallituksiin. EU tukee pyrkimyksiä määritellä verkossa toimimiselle normeja, joihin kaikkien sidosryhmien tulisi sitoutua. EU odottaa kansalaistensa kunnioittavan kansalaisvelvollisuuksia, yhteiskunnallisia vastuita ja lakeja verkossakin, ja niin myös valtioiden olisi sitouduttava normeihin ja voimassa oleviin lakeihin. Kansainväliseen turvallisuuteen liittyvissä kysymyksissä EU kannattaa luottamusta lujittavia toimia

[30] *Yritysten yhteiskuntavastuuta koskeva uudistettu EU:n strategia vuosiksi 2011–2014*, KOM(2011) 681 lopullinen.

kyberturvallisuuden alalla läpinäkyvyyden lisäämiseksi ja jotta voitaisiin vähentää sitä riskiä, että valtioiden toimintatavoista syntyisi väärä käsitys.

EU ei kannata uusien kansainvälisten säädösten luomista verkkokysymyksissä.

Kansalaisoikeuksia ja poliittisia oikeuksia koskevassa kansainvälisessä yleissopimuksessa, Euroopan ihmisoikeussopimuksessa ja EU:n perusoikeuskirjassa asetettuja oikeudellisia velvoitteita olisi kunnioitettava myös verkkoympäristössä. EU keskittyykin siihen, miten näiden velvoitteiden noudattaminen voitaisiin varmistaa myös kyberavaruudessa.

Verkkorikollisuuden osalta taas Budapestin sopimus on sääntelyväline, johon kolmannetkin maat voivat vapaasti sitoutua. Se toimii mallina kansalliselle verkkorikoslainsäädännölle ja perustana alan kansainväliselle yhteistyölle.

Jos aseelliset konfliktit leviävät verkon puolelle, sovelletaan kansainvälistä humanitaarista oikeutta ja tilanteen mukaan ihmisoikeuslainsäädäntöä.

Kyberturvallisuuteen ja vakaisiin tietoinfrastruktuureihin liittyvien valmiuksien kehittäminen kolmansissa maissa

Lisääntyvä kansainvälinen yhteistyö tukee viestintäpalvelujen perustana olevien infrastruktuureiden sujuvaa toimintaa. Yhteistyöhön kuuluu parhaiden käytänteiden levittämistä, tiedonvaihtoa, yhteisiä varhaisvaroitusharjoituksia jne. EU tukee kehitystä tehostamalla meneillään olevaa kansainvälistä työtä hallitusten ja yksityisen sektorin yhteistyöverkostojen lujittamiseksi kriittisten tietoinfrastruktuurien suojaamisen alalla.

Kaikkialla maailmassa ei päästä hyötymään internetin myönteisistä vaikutuksista, koska saatavilla ei ole avoimia, turvallisia, yhteentoimivia ja luotettavia liityntämahdollisuuksia. Tästä syystä Euroopan unioni tukee jatkossakin maiden pyrkimyksiä kehittää liityntämahdollisuuksia ja internetin käyttöä niiden kansalaisten keskuudessa, jotta voidaan varmistaa verkon eheys ja tietoturvallisuus ja torjua käytännössä verkkorikollisuutta.

Yhteistyössä jäsenvaltioiden kanssa komissio ja korkea edustaja

- pyrkivät johdonmukaiseen EU:n kansainväliseen verkkotoimintapolitiikkaan lisätäkseen yhteydenpitoa keskeisten kansainvälisten kumppanien ja organisaatioiden kanssa, sisällyttääkseen verkkokysymykset yhteiseen ulko- ja turvallisuuspolitiikkaan ja parantaakseen koordinointia maailmanlaajuisissa verkkokysymyksissä;
- tukevat kyberturvallisuusalan toimintanormien ja luottamusta lujittavien toimien kehitystä; helpottavat vuoropuhelua voimassa olevan kansainvälisen oikeuden soveltamisesta verkossa ja edistävät Budapestin sopimusta verkkorikollisuuden torjumiseksi,
- tukevat perusoikeuksien, kuten tiedonsaantioikeuden ja ilmaisunvapauden, edistämistä ja suojaa keskittymällä seuraaviin: a) uusien julkisten ohjeistojen laatiminen ilmaisunvapaudesta verkossa ja reaalimaailmassa, b) sellaisten tuotteiden ja palvelujen viennin seuranta, joita voitaisiin käyttää sensurointiin tai joukkovalvontaan verkossa, c) toimenpiteiden ja välineiden kehittäminen internetin saatavuuden, avoimuuden ja vakauden lisäämiseksi, jotta voidaan puuttua viestintäteknologiaa hyödyntävään sensurointiin tai joukkovalvontaan, d) eri sidosryhmien valtaistaminen viestintäteknologian käytössä

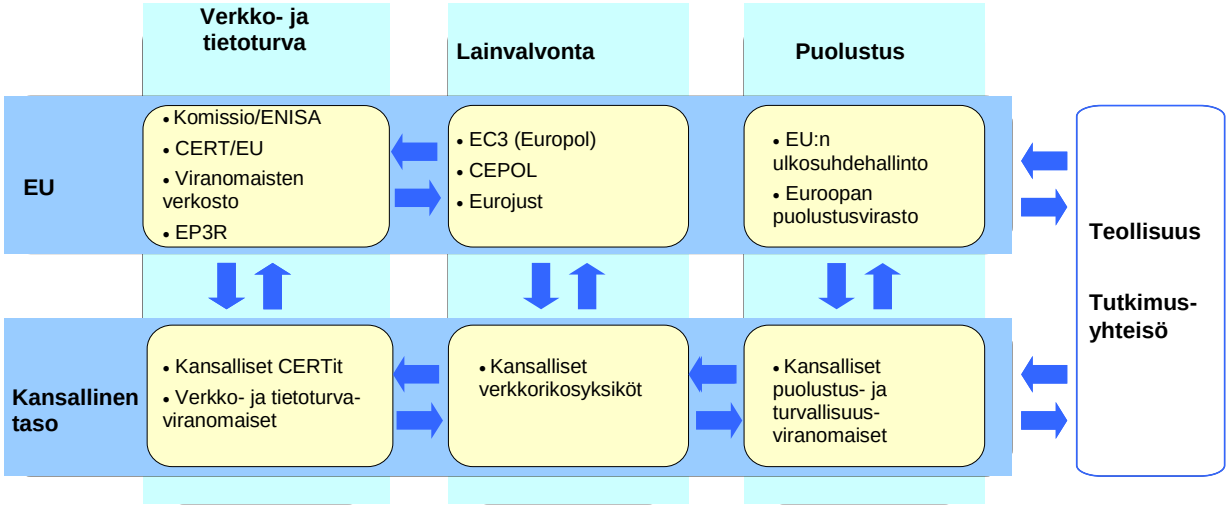
perusoikeuksien edistämiseksi,

- tukevat kansainvälisten kumppanien ja organisaatioiden, yksityisen sektorin ja kansalaisyhteiskunnan kanssa maailmanlaajuista valmiuksien kehittämistä kolmansissa maissa tiedonsaannin parantamiseksi, internetin avaamiseksi, verkkouhkien, kuten tahattomien häiriöiden, verkkorikollisuuden ja verkkoterrorismin, ehkäisemiseksi ja torjumiseksi sekä rahoittajatahojen koordinoimiseksi valmiuksien kehittämistoiminnan suuntaamisessa,
- hyödyntävät EU:n eri tukijärjestelmiä kyberturvallisuusvalmiuksien parantamiseen, mukaan luettuna verkkouhkiin liittyvä lainvalvonta- ja oikeusviranomaisten sekä teknisen henkilöstön koulutus; tukevat tarvittavien kansallisten toimintapolitiikkojen, strategioiden ja instituutioiden luomista kolmansissa maissa,
- lisäävät politiikan koordinointia ja tiedonvaihtoa kansainvälisissä kriittisten tietoinfrastruktuurien suojaamista käsittelevissä verkostoissa, kuten Meridian-verkostossa, ja lisäävät yhteistyötä verkko- ja tietoturva-alan toimivaltaisten viranomaisten ja muiden viranomaisten keskuudessa.

3. ROOLIT JA VASTUUT

Verkon uhat eivät tunne maantieteellisiä rajoja verkottuneessa digitaalitaloudessa ja yhteiskunnassa. Kaikkien toimijoiden, kuten verkko- ja tietoturva-alan viranomaisten, CERT-ryhmien, lainvalvontaviranomaisten ja elinkeinoelämän on kannettava vastuunsa sekä kansallisesti että EU-tasolla ja yhdessä lujitettava kyberturvallisuutta. Koska asiaan voi liittyä erilaisia oikeudellisia puitteita ja toimivaltakysymyksiä, EU:n keskeisenä haasteena on selventää lukuisien asiaan liittyvien toimijoiden rooleja ja vastuita.

Koska kysymys on hyvin monimutkainen ja asiaan liittyy niin monenlaisia toimijoita, keskitetty Euroopan tasoinen ohjaus ei tule kyseeseen. Kansallisilla hallituksilla on parhaat mahdollisuudet organisoida verkon turvallisuuspoikkeamien ja verkkohyökkäysten ehkäisy ja niihin reagointi sekä luoda yhteydet ja verkostot yksityisen sektorin ja suuren yleisön kanssa niiden vakiintuneiden poliittisten kanavien ja oikeudellisten puitteiden kautta. Riskien potentiaalisen tai todellisen maiden rajojen yli ulottuvan luonteen vuoksi tuloksellinen kansallinen vastatoiminta edellyttäisi monissa tapauksissa EU-tason tukea. Jotta kyberturvallisuutta voitaisiin edistää kattavasti, toiminnan olisi jakauduttava kolmen toimialan kesken: verkko- ja tietoturva, lainvalvonta ja puolustus. Nämä alat toimivat myös erilaisissa oikeudellisissa puitteissa:



3.1. Toimivaltaisten verkko- ja tietoturvaviranomaisten/CERT-ryhmien, lainvalvontaviranomaisten ja puolustusviranomaisten koordinointi

Kansallinen taso

Jäsenvaltioilla olisi oltava jo nyt tai tämän strategian seurauksena rakenteet, joiden avulla ne pystyvät käsittelemään verkkojen sietokykyä, verkkorikollisuutta ja puolustusta. Rakenteiden olisi saavutettava tarvittavat valmiudet selviytyä verkkoturvapoikkeamista. Koska useilla tahoilla voi kuitenkin olla operatiivisia vastuita kyberturvallisuuden eri ulottuvuuksien suhteen ja koska yksityisen sektorin osallistuminen on erittäin tärkeää, kansallisen tason koordinointi olisi optimoitava eri ministeriöiden välillä. Jäsenvaltioiden olisi kansallisissa kyberturvallisuusstrategioissaan määriteltävä eri kansallisten tahojen roolit ja vastuut.

Tiedonvaihtoa kansallisten tahojen kesken ja yksityisen sektorin kanssa olisi kannustettava, jotta jäsenvaltioilla ja yksityisellä sektorilla olisi kaiken aikaa kokonaiskuva eri uhkatekijöistä ja parempi ymmärrys uusista suuntauksista ja tekniikoista, joita käytetään verkkohyökkäyksissä tai joilla voidaan reagoida niihin nykyistä nopeammin. Luomalla kansallisen verkko- ja tietoturvan yhteistyösuunnitelman verkkoturvallisuuspoikkeamatilanteita varten jäsenvaltiot voisivat selkeästi kohdentaa roolit ja vastuut ja optimoida toiminnan poikkeamatilanteessa.

EU:n taso

Kuten kansallisellakin tasolla, myös EU:n tasolla kyberturvallisuuteen liittyy monia toimijoita. Verkko- ja tietoturvan, lainvalvonnan ja puolustuksen näkökulmasta aktiivisia toimijoita ovat erityisesti ENISA, Europol/EC3 ja EDA. Jäsenvaltiot ovat edustettuina niiden hallintoneuvostoissa ja ne tarjoavat puitteet EU-tason koordinoinnille.

ENISAa, Europolia/EC3:a ja EDAa kannustetaan koordinointiin ja yhteistyöhön aloilla, joilla ne toimivat yhdessä, erityisesti trendianalyysien, riskinarviointien, koulutuksen ja parhaiden käytäntöjen jakamisen osalta. Niiden olisi tehtävä yhteistyötä säilyttäen kuitenkin omat erityispiirteensä. Näiden virastojen olisi yhdessä CERT-EU-ryhmän, komission ja jäsenvaltioiden kanssa tuettava tämän alan teknisten ja toimintapoliittisten asiantuntijoiden luotetun yhteisön kehittymistä.

Epävirallisia koordinointi- ja yhteistyökanavia täydennetään jäsennellymmillä yhteyksillä. EU:n sotilashenkilöstöä ja EDAn kyberpuolustus-projektiryhmää voidaan käyttää

koordinointiin puolustusalalla. Europolin/EC3:n ohjelmaryhmässä kokoontuvat muun muassa EUROJUST, CEPOL, jäsenvaltiot[31], ENISA ja komissio ja se tarjoaa mahdollisuuden jakaa eri osapuolten erityisosaamista ja varmistaa, että EC3:n toimet toteutetaan yhdessä niin, että kaikkien osapuolten asiantuntemus tunnustetaan ja toimivaltuuksia kunnioitetaan. ENISAn uusi toimeksianto mahdollistanee yhteydenpidon lisäämisen Europolin sekä teollisuuden sidosryhmien kanssa. Verkko- ja tietoturvaa koskevan komission lainsäädäntöehdotuksen mukaisesti luotaisiin yhteistyöverkosto, joka koostuisi kansallisista toimivaltaisista verkko- ja tietoturvaviranomaisista. Ehdotuksessa käsitellään myös tiedonvaihtoa verkko- ja tietoturvaviranomaisten ja lainvalvontaviranomaisten välillä.

Kansainvälinen taso

Komissio ja korkea edustaja varmistavat yhdessä jäsenvaltioiden kanssa, että kyberturvallisuuden alalla toimitaan kansainvälisellä tasolla koordinoidusti. Tässä yhteydessä komissio ja korkea edustaja ylläpitävät EU:n perusarvoja ja edistävät verkkoteknologioiden rauhanomaista, avointa ja läpinäkyvää käyttöä. Komissio, korkea edustaja ja jäsenvaltiot osallistuvat poliittiseen vuoropuheluun kansainvälisten kumppanien ja kansainvälisten organisaatioiden, kuten Euroopan neuvosto, OECD, ETYJ, NATO ja YK, kanssa.

3.2. EU:n tuki mittavan verkkoturvallisuuspoikkeaman tai verkkohyökkäyksen aikana

Suurilla verkkoturvallisuuspoikkeamilla tai verkkohyökkäyksillä on todennäköisesti vaikutuksia hallinnoille, yrityksille ja yksityishenkilöille EU:ssa. Tämän strategian ja erityisesti verkko- ja tietoturvaa koskevan direktiiviehdotuksen myötä verkkoturvallisuuspoikkeamien ennaltaehkäisyn, toteamisen ja niihin reagoimisen on määrä parantua ja jäsenvaltiot ja komissio pitänevät toisensa tiiviimmin ajan tasalla mittavista verkkoturvallisuuspoikkeamista tai verkkohyökkäyksistä. Reagointimekanismit kuitenkin vaihtelevat poikkeaman luonteen, mittakaavan ja rajat ylittävyyden mukaan.

Jos poikkeama vaikuttaa vakavasti toiminnan jatkuvuuteen, ehdotetun verkko- ja tietoturvadirektiivin mukaan aletaan noudattaa kansallista tai unionin verkko- ja tietoturvan yhteistyösuunnitelmaa sen mukaan, vaikuttaako poikkeama maiden rajojen yli. Toimivaltaisten verkko- ja tietoturvaviranomaisten verkostoa käytettäisiin tässä yhteydessä tiedonvaihtoon ja tuen antamiseen. Tämä mahdollistaisi kohteena olevien verkkojen ja palvelujen suojaamisen ja/tai toimintakuntoon palauttamisen.

Jos poikkeama näyttäisi liittyvän rikollisuuteen, siitä olisi ilmoitettava Europolille ja EC3:lle, jotta ne voivat yhdessä kohdemaiden lainvalvontaviranomaisten kanssa käynnistää tutkinnan, tallentaa todisteet, tunnistaa epäillyt ja lopulta varmistaa, että epäillyt asetetaan syytteeseen.

Jos poikkeama näyttäisi liittyvän verkkovakoiluun tai valtion rahoittamaan hyökkäykseen tai sillä on vaikutuksia kansalliseen turvallisuuteen, kansalliset turvallisuus- ja puolustusviranomaiset varoittavat muita vastaavia viranomaisia hyökkäyksen kohteeksi joutumisesta, jotta nämä pystyvät puolustautumaan. Tämän jälkeen käynnistetään varhaisvaroitusmekanismit ja tarvittaessa kriisinhallinta- ja muut menettelyt. Poikkeuksellisen vakava verkkoturvallisuuspoikkeama tai verkkohyökkäys voisi antaa jäsenvaltiolle riittävät perusteet tukeutua EU:n yhteisvastuulausekkeeseen (Euroopan unionin toiminnasta tehdyn sopimuksen 222 artikla).

[31] Edustettuina tietoverkkorikollisuutta käsittelevässä erityisryhmässä (Cybercrime Task Force), joka koostuu jäsenvaltioiden verkkorikosyksiköiden johtajista.

Jos poikkeama näyttäisi murtaneen henkilötietojen suojan, siitä olisi ilmoitettava kansallisille tietosuojaviranomaisille tai direktiivin 2002/58/EY mukaiselle kansalliselle sääntelyviranomaiselle.

Verkkoturvallisuuspoikkeamien ja verkkohyökkäyksien käsittelyssä on hyötyä yhteydenpitoverkostoista ja kansainvälisten kumppanien avusta. Tässä yhteydessä voi olla kyse seurausten teknisestä lieventämisestä, rikostutkinnasta tai kriisinhallintamekanismien käynnistämisestä.

4. PÄÄTELMÄT JA JATKOTOIMET

Tässä komission ja unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan ehdotuksessa Euroopan unionin kyberturvallisuusstrategiaksi hahmotellaan EU:n visio ja tarvittavat toimet, joilla pyritään kansalaisten oikeuksien vahvaan suojaamiseen ja edistämiseen niin, että EU:n verkkoympäristöstä tulisi maailman turvallisin[32].
Tämä visio voidaan toteuttaa ainoastaan monien toimijoiden todellisella kumppanuudella ottamalla vastuu ja kohtaamalla tulevat haasteet.
Näin ollen komissio ja korkea edustaja pyytävät neuvostoa ja Euroopan parlamenttia hyväksymään tämän strategian ja auttamaan toteuttamaan hahmotellut toimet. Vahvaa tukea ja sitoutumista tarvitaan myös yksityiseltä sektorilta ja kansalaisyhteiskunnalta, jotka ovat avaintoimijoita parannettaessa turvallisuustasoa ja turvattaessa kansalaisten oikeuksia.

Toiminnan aika on nyt. Komissio ja korkea edustaja ovat päättäneet ryhtyä yhteistyöhön kaikkien toimijoiden kanssa tarvittavan turvallisuuden luomiseksi Eurooppaan. Varmistaakseen, että strategia pannaan täytäntöön ilman viivytyksiä ja jotta sitä voidaan arvioida suhteessa mahdollisiin uusiin kehityskulkuihin, ne kokoavat kaikki asiaankuuluvat tahot korkean tason konferenssiin ja arvioivat edistymistä 12 kuukauden kuluttua.

[32] Strategia rahoitetaan kunkin politiikkalohkon (Verkkojen Eurooppa -väline, Horisontti 2020, sisäisen turvallisuuden rahasto, yhteinen ulko- ja turvallisuuspolitiikka ja ulkoinen yhteistyö, erityisesti vakautusväline) ennakoitujen määrärahojen puitteissa, siten kuin ne on esitetty komission ehdotuksessa monivuotiseksi rahoituskehykseksi 2014–2020 (jollei budjettiviranomaisen päätöksestä muuta johdu ja riippuen hyväksytyn vuosien 2014–2020 rahoituskehyksen lopullisista määrärahoista). Mitä tulee tarpeeseen varmistaa kokonaisyhteensopivuus erillisvirastojen käytettävissä olevien virkojen ja seuraavassa monivuotisessa rahoituskehyksessä erillisvirastoille kussakin menoluokassa osoitettavien määrärahojen kanssa, virastoja (CEPOL, EDA ENISA, EUROJUST ja EUROPOL/EC3), joita pyydetään tässä tiedonannossa ottamaan hoitaakseen uusia tehtäviä, kannustetaan tekemään niin siinä määrin kuin viraston mahdollisuudet saada lisää resursseja ovat tiedossa ja kaikki uudelleenjärjestelymahdollisuudet on selvitetty.