

ECT FORUM 09

Valtakunnansyyttäjä Matti Kuusimäki 23.9.2009

HÄMÄHÄKKEJÄ VERKOSSA

Tietoverkkorikollisuuden torjunta syyttäjän näkökulmasta

JOHDANTOA

Tietoverkkoon kohdistuva rikollisuus

Tietoliikenteen, tietokoneiden, tietojärjestelmien sekä näihin kytkettyjen oheislaitteiden ja tietoverkon tarjoamien palveluiden häiritsemisellä tai niiden lainvastaisella hyväksikäytöllä tavoitellaan taloudellista tai muuta hyötyä, esimerkiksi poliittisen, ideologisen tai uskonnollisen päämäärän toteuttamiseksi. Laiton hyväksikäyttö ilmenee mm. tietoa hankkimalla (kaappaamalla, murtautumalla) ja hyväksikäyttämällä, muuntamalla tai vääristämällä sekä tietoliikennettä häiritsemällä ruuhkauttaen tai sulkien tietoliikenteen toiminnan. Laiton toiminta voi kohdistua luonnolliseen henkilöön, yhteisöön, julkiseen ja yksityiseen sektoriin tai jopa koko yhteiskuntaan.

Tietoverkkoon itseensä kohdistuvat rikokset ovat pääsääntöisesti luokiteltavissa tieto- ja viestintärikoksiksi sekä yleisvaarallisiksi rikoksiksi. Teknologian kehityksen ja tietoverkon yleistymisen myötä rikoslakiin on tullut tarve lisätä rikosnimikkeitä, jotka ilmentävät tietoverkkoon kohdistuvia rikoksia kuten vaaran aiheuttaminen tietojenkäsittelylle, tietoverkkorikosvälineen hallussapito, tietoliikenteen- tai tietojärjestelmän häirintä sekä suojauksen purkujärjestelmärikos. Kuten rikosnimikkeiden ulkoasusta voidaan päätellä, eivät tällaiset lainvastaiset teot sisältyneet rikoslakiin esimerkiksi vielä silloin, kun väritelevisio teki tuloaan Suomeen. Toisaalta esimerkiksi perinteiset ilkivalta-, vahingonteko-, luvaton käyttö- sekä murtovälineen hallussapitorikokset ovat

nekin peruseriaatteiltaan hyvin samankaltaisia tietoverkkoon kohdistuvien nykyisten tekojen luonteen kanssa.

Tietoverkossa tapahtuva rikollisuus

Tietoverkossa tapahtuva laitton toiminta edustaa usein aivan perinteistä rikollisuutta. Tyypillisimmillään rikokset ovat omaisuuden kohdistuvia petos-, maksuväline-, varkaus- ja kavallusrikkoksia.

Uutta sen sijaan on esimerkiksi se, että poliisille on alkanut tulla tutkintapyyntöjä myös virtuaalimaailmasta, esimerkiksi Habbo-hotellin asunnon huonekalujen katoamistapauksia koskevia.

Rekisteröityminen virtuaalimaailmaan sekä omaisuuden hankkiminen siellä ovat maksullista toimintaa. Rekisteröityneiden henkilöiden käyttäjätunnuksia varastamalla tai lainaamalla virtuaalimaailman rahanarvoista omaisuutta on saatettu siirtää pelaajalta toiselle. Teot ovat tunnusmerkistöltään verrattavissa varkaus- tai kavallusrikkoksiin. Anastetun omaisuuden arvoa mitattaessa tapaukset ovat tähän asti olleet sangen vaatimattomia. Mutta globaalisti tarkasteltuna virtuaalimaailman pelit ovat miljardiluokan liiketoimintaa, jossa pelimaailman omaisuus tai status voi olla arvokastakin kauppatavaraa.

Tietoverkkoa hyväksikäyttävä rikollisuus

Tietoverkkoa välineenä hyödynnetään rikollisissa yhteyksissä samalla tavoin kuin jokapäiväisessä käytössä, toisin sanoen rikollisten välisessä yhteydenpidossa, hankittaessa rikoksen tekoon tarvittavia välineitä tai palveluita, hankittaessa tietoa mahdollisista kohteista tai hankittaessa tietoa viranomaisten toiminnasta.

Ja maailma pienenee. Tietoverkko on verraton apu kansainväliselle laittomalle toiminnalle, erityisesti huumausainerikollisuuden, laittoman maahantulon järjestämisen, paritusrikosten, ihmiskaupan sekä rahanpesurikosten ollessa kysymyksessä

Suomessa seksipalveluiden markkinointia ei sanomalehdissä nykyisin näe, eikä katuprostitutiota ilmene, yksittäistapauksia lukuun ottamatta. Sen sijaan internet toimii tehokkaana prostituutiomarkkinoiden rekrytointi-, markkinointi- ja tiedonvaihtokanavana. Toimintaa ohjataan ulkomailta, usein Euroopan ulkopuolella sijaitsevien palvelinten avulla. Palvelinten fyysisen sijainnin vuoksi Suomen viranomaisten puuttuminen toimintaan on hankalaa, usein jopa mahdotonta, mikäli sijaintipaikan lainsäädäntö ei pidä seksin verkkomarkkinointia rikoksena.

Laittoman maahantulon järjestämisessä internetin hyödyt ovat ilmenneet usealla tavalla. Tyypillistä on, että varastettuja luottokorttitietoja hyödyntäen tilataan lentolippuja henkilöille, jotka matkustavat väärän henkilöllisyyden turvin ja ylittävät laittomasti useamman valtion rajan. Väärää matkustusidentiteettiä saatetaan käyttää myös kirityskeinona siten, että laittomasti maassa oleskeleva henkilö alistetaan myymään seksipalveluita tai tekemään muunlaista pakkotyötä.

Tietoverkon massalevitysominaisuudet ovat olleet omiaan mullistamaan esimerkiksi tekijänoikeusrikosten sekä lainvastaisen kuvamateriaalin hallussapidon, esittämisen ja levittämisen.

Laiton materiaali saattaa koostua kymmenistä tai jopa sadoista tuhansista kappaleista ja tiedon kokoluokkaa mitataan giga- tai tera-asteikolla. Siinä missä musiikki tai elokuvataltioiden laitton kopiointi ja levitys saattoi ennen olla sangen rajattua poikaporukan puuhastelua, on se tietoverkkojen tehokkaan levityskyvyn myötä laajentunut kansainväliseksi ja ilmeisen kannattavaksi bisnekseksi. Toiminnan aiheuttamat vahingot voivat olla valtavia. Sitä paitsi voi jopa sattua, että esimerkiksi verkkoon ladattu lapsipornomateriaali säilyy tietoverkossa ikiajat.

Lapsipornon levityksen lisäksi lapsen seksuaalisen hyväksikäytön muut muodot ovat moninaistuneet tietoverkon kehittyessä. Erilaiset chat -palstat mahdollistavat anonyymien tai harhauttavan

profiilin turvin kontaktien luomisen aikuisen ja lapsen välillä. Kuvan ja videon tehokkaamman siirtokyvyn myötä lapsen seksuaalista hyväksikäyttöä pystytään toteuttamaan ”etänä”.

TIETOVERKKORIKOLLISUUS TÄNÄÄN JA HUOMENNA

Maksukorttirikollisuus

Maksukorttirikollisuus näyttää jo nyt olevan korkealuokkaista teknologiaa tehokkaasti hyödyntävää kansainvälistä ja järjestäytynyttä. Tietoverkossa toimivaa maksukorttirikollisuutta pidetäänkin eräänä merkittävimmistä petosrikollisuuden uusista uhkista. Verrattaessa esimerkiksi heinäkuun 2008 ja heinäkuun 2009 rikostilastoja maksuvälinerikollisuuden kasvu on miltei kaksinkertaistunut.

Maksukorttirikollisuuden voi otaksua edelleen kasvavan kansallisten maksujärjestelmien poistussa. Suomikin on liittymässä lähes koko Euroopan kattavaan yhtenäisen euromaksualueeseen eli ns. SEPA-alueeseen (Single Euro Payments Area). Suomalaisten pankkien ja luottolaitosten myöntämät maksukortit tulevat toiminaan koko SEPA-alueella. Silloin Suomesta tulee muiden Euroopan maiden tavoin houkutteleva maa myös korttirikollisten näkökulmasta.

Maksukorttidataa kaapataan tietoverkossa joko huonosti suojatuista verkkopalveluista tai huonosti suojatun kotikoneen kautta kotikoneen käyttäjän syöttäessä maksukorttitiedot verkkomakkeelle. Luottokorttinumeroiden ohella helposti rahaksi muutettavaa identiteettitietoa ovat verkkokauppatunnukset.

Yhdysvalloissa jäi äskettäin kiinni tekijä, joka oli saanut haltuunsa 130 miljoonaa luottokorttinumeroa. Tekijän toteuttama isku kohdistui pankin ja kaupan välissä maksujen välittäjänä toimivan yrityksen palvelimeen. Tällaiset palveliniskut eivät ole onneksi yleisiä, koska järjestelmät ovat yleensä hyvin suojattuja. Mikäli operaatio kuitenkin onnistuu, on saaliskin suuri.

Vuonna 2008 Suomessakin paljastui operaatio, jossa suomalaisen pankin asiakkaiden verkkopankkitunnuksia onnistuttiin kaappaamaan perättömän ”Ydinvoimalaonnettomuus Mikkelissä” - uutisen avulla. Uutissivustolla käyneiden henkilöiden koneisiin asentui haittaohjelma, jonka avulla rikolliset pääsivät soluttautumaan verkkopankin kirjautumistapahtumaan siten, että henkilön pankkitililtä pysyttiin tekemään rahansiirtoja. Rikollisten interventio onnistui niissä tapauksissa, joissa tietokoneet olivat huonosti suojatut. Kokonaisvahinko jäi onneksi vain 30 000 euroon.

Suomessa pankkirikoksissa vahingot ovat ylipäättäänkin olleet pieniä verrattuna Aasiaan, Yhdysvaltoihin ja Keski-Eurooppaan. Esimerkiksi Britanniassa vuonna 2007 vahingot verkkopankkeihin kohdistuneissa rikoksissa olivat lähes 30 miljoonaa euroa, Suomen vastaavan luvun ollessa vain 60 000 euron luokkaa.

”Muulien” käyttö verkkokaupassa

Kun rikollinen on saanut haltuunsa suuren määrän luottokorttitietoja, niitä käytetään esimerkiksi kalliin tavarahan, kuten elektroniikan, ostamiseen verkkokaupoista. Jotta kiinnijäämisriski olisi mahdollisimman pieni, ostotapahtuman ja tavarahan vastaanottamisen sekä edelleen lähettämisen hoitavat ennalta rekrytoidut henkilöt eli ns. muulit.

Muulien tehtävänä on ostaa verkkokaupasta tavaraa ja ottaa ne vastaan kotiosoitteeseensa. Vastaanotetut tavarat lähetetään edelleen, yleensä johonkin kolmanteen maahan, jotta ketjun seuraaminen olisi viranomaiselle mahdollisimman hankalaa. Muuleja rekrytoidaan Suomestakin jo aivan säännöllisesti. Rekrytoijat pyrkivät näin pitämään yllä käsitystä laillisesta työpaikasta.

Yritys- ja liikesalaisuuksiin kohdistuvat hyökkäykset

Tieto on tänä päivänä suurelle osalle elinkeinoelämää keskeinen tekijä. Yritysten tietopääomas- ta ovat kiinnostuneet niin kilpailijat kuin tietoverkossa toimivat palkkionmetsästäjätkin. Palk- kionmetsästäjät voivat myydä hankkimansa tiedon siitä parhaiten maksavalle taholle, onpa se sitten itse yritys, jolta tieto on anastettu, kilpailija tai toinen palkkionmetsästäjä. Kiristämisri- koskin on tässä touhussa nurkan takana.

Tietoturvallisuuden ylläpito ei ole pelkästään päivitettyjen suojausohjelmien käyttöä tai tieto- turvakäytänteiden noudattamista. Virustorjuntaan ja palomuureihin perustuva suojautumismalli kykenee havaitsemaan ennalta tunnettuja haittaohjelmia. Yritysvakoilija lähettää kuitenkin mil- tei varmuudella tunnistamattoman haittaohjelman. Jos suojautuminen on jätetty virustorjunnan varaan, yritys on haavoittuva. Järjestäytyneen rikollisuuden on havaittu myös pyrkivän entistä aktiivisemmin verkottumaan tai rekrytoitumaan aivan lailliseen liiketoimintaan sekä julkisen sektorin palvelukseen. Suomessa laittoman tiedonhankinnan on havaittu kohdistuvan erityisesti korkean teknologian sektorin yrityksiin, kuten bio- ja lääketieteeseen, energiatuotantoon sekä informaatioteknologiaan.

YLEISIÄ VÄÄRINKÄYTÖSILMIÖITÄ

Verkkourkinta eli phishing

Verkkorikosten esiteko on usein sellaisen tiedon haltuunotto, jota voi hyödyntää taloudellisen edun hankkimiseksi. Klassisin keino kaapata tietoa on huijata ihminen kertomaan tieto jonkin peitetarinan avulla, kuten pankin nimissä lähetetyllä tietoturvakyselyllä. Suomessa käyttäjätun- nuksien ja salasanojen massiivista urkintaa on kohdistunut mm. pankkien asiakkaisiin. Toiminnan jäljet ovat pääsääntöisesti johtaneet Euroopan ulkopuolelle. Suomessa verkkourkinta on kuiten- kin ollut melko marginaalinen uhka, koska pankkiemme turvallisuusjärjestelmä on ainakin tähän asti ollut varsin hyvä.

”Identiteettivarkaudet”

Näiden tekojen arvellaan olevan yksi nopeimmin kasvavista rikollisuuden muodoista. Väärän identiteetin avulla toteutetussa petosrikostyyppisessä teossa uhrin asemassa nähdään yleensä harhautettu ostaja tai myyjä. Sen sijaan henkilö, jonka identiteettiä on käytetty luvattomasti rikollisessa toiminnassa, jää usein tarkastelun ulkopuolelle.

Identiteetin luvaton käyttö tulisi voida huomioida lainsäädännössämme paremmin. Kaapattuja identiteettejä käytetään hyväksi ennen muuta maksuvälinepetoksissa ja laittoman maahantulon järjestämisessä. Koska kaappausta sellaisenaan ei ole kriminalisoitu, poliisi pääsee puuttumaan asiaan vasta käytettäessä tietoa hyväksi jonkin rikoksen toteutuksessa. Tällöin alkuperäistä tietoteknistä jälkeä ei enää ole tallella.

Bot-verkot (robottiverkko, botnet)

Bot-verkko on eräänlainen rikollisten ”Sveitsin armeijan linkkari”, jota on havaittu käytettävän apuna lähes kaikessa laajamittaisessa verkkorikollisuudessa. Bot-verkko voi koostua sadoista tai jopa sadoista tuhansista kaapatuista kotitietokoneista muodostaen rikollisten etäohjaaman verkon, jota voidaan käyttää hyväksi anonyymisti ja lähes ilmaiseksi. Kotitietokoneen omistajan näkökulmasta tällainen toiminta jää usein havaitsematta. Yksittäisenä tekona arvioiden tietokoneen kaappaaminen voi olla näennäisen lievä oikeudenloukkaus, mutta kokonaisuutta tarkastellen toiminta voi aiheuttaa todella vakavia ja laaja-alaisia vahinkoja. Viime aikoina identiteettitiedon kaappaaminen on siirtynyt tietoverkon palveluista selkeästi tietoverkkoasioinnin asiakaspäähän. Tieto kaapataan bot-verkon osaksi valjastetuilta koneilta silloin, kun koneen todellinen haltija kirjautuu verkkokauppaan tai -pankkiin. Viestintäviraston arvion mukaan Suomessa on jatkuvasti noin 1000 - 1500 tietokonetta kaapattuna bot-verkkoon.

Palvelunestohyökkäykset

Tyypillinen bot-verkon avulla toteutettu operaatio Suomessa oli todistettavissa varsin äskettäin Suomessa, kun Veikkaus Oy:n nettipalvelin ruuhkautettiin kesken lauantai-illan pelien. Erityisesti brittiläisiin ja yhdysvaltalaisiin vedonlyöntifirmoihin kohdistuvat hyökkäykset ja hyökkäyksiin liittyvä kiristys olivat joitain vuosia sitten näkyvä ilmiö.

Palvelunestohyökkäysilmiön ei odoteta leviävän Suomeen samassa mittakaavassa, sillä rikoksen tuotto-riski-suhde on verraten huono. Kiristäjät joutuvat ottamaan rahaa fyysisesti vastaan, jolloin heidän jäljittämisenä on helpompaa. Verkko- ja verkkohyökkäys myös estää saman rikollisen infrastruktuurin käyttämisen paljon tuottoisampaan tietokaappaukseen.

TIETOVERKKORIKOLLISUUDEN TORJUNTA

Vaikealta saattaa näyttää, mutta eipä heitetä vielä hanskoja tiskiinkin. Tietoverkkorikollisuus ei ole suinkaan 2000-luvun keksintö. Nykypäivän kaltaisia tietomurtoja on Suomessa tutkittu ensimmäisen kerran jo 1980 - luvulla. Tietoverkkorikollisuuden taustamotivaatiot ja ideologia eivät juuri poikkea perinteisemmästä rikollisuudesta. Tietoverkkorikollisuutta torjutaan samoin keinoin eli uutta teknologiaa ja menetelmiä hyväksi käyttäen. Rikostutkinta ja rikosoikeudenhoito kokonaisuudessaan kehittyvät nekin kokemuksen ja kehitystyön myötä.

Koulutus

Tietoverkkorikostenkin esitutkinnasta ja sen kehitystyöstä vastaa pääosin poliisi. Tietoverkkorikollisuus on huomioitu jo poliisiin perusopetuksessa. Poliisiammattikorkeakoulussa annetaan lisäksi syventävää koulutusta mm. tietotekniseen rikostutkintaan sekä digitaalisen todistusaineiston käsittelyyn. Syyttäjälaitos tekee tiivistä yhteistyötä poliisin kanssa ja järjestää syyttäjille räätälöityä koulutusta syyttäjäakatemiassaan. Juuri nytkin on kurssi meneillään. Tietoverkkorikollisuus on muutoinkin yksi syyttäjätöiminnan painopistealueista. Tietoverkkorikoksiin erikoistuneet avainsyyttäjät pyrkivät paneutumaan substanssialueensa tapauksiin sekä perehtymään

juttujensa ohella myös pintaa syvemmälle tietoverkon yleisiin ilmiöihin ja kehitystrendeihin. Heidän tehtävänä on sitten valtakunnallisen palvelujaon mukaisesti konsultoida ympäri maan muita syyttäjiä uusissa ongelmatilanteissa.

Kansainvälinen yhteistyö

Tämän päivän rikostutkinnassa kansainvälisen yhteistyön merkitys on vallannut yhä suuremman roolin, tutkittiinpa sitten omaisuus-, huumausaine- tai tietoverkkorikoksia. Tietoverkkorikollisuuden tutkinnassa kansainvälisen yhteistyön merkitys on aivan keskeistä. Keinoja siihen on useita.

Europol

Euroopan unionin poliisiviraston Europolin toiminta on osa EU-yhteistyötä. Sen avulla tehostetaan kansainvälistä rikostorjuntaa. Yleinen tiedonvaihto, tietoverkkoilmiöiden tarkastelu, juttujen sarjoittaminen, hyväksi havaittujen rikostutkimusmenetelmien jakaminen sekä rikostutkinnan tuki monikansallisissa tapauksissa kuuluvat Haagissa sijaitsevan Europolin työkalupakkiin.

Eurojust

Unionimaiden syyttäjäviranomaisten edustajista koostuvan Eurojustin toiminnan tavoitteena on edistää tutkinta- ja syytetoimien koordinoitua Euroopan unionin jäsenvaltioiden välillä, vakavan rajat ylittävän ja järjestäytyneen rikollisuuden torjumiseksi. Eurojustin rooli korostuu ennen muuta usean valtion välisiä toimivaltuuskysymyksiä ratkottaessa. Eurojust voi erityistapauksessa Haagista käsin tukea rikostutkintaa myös Euroopan ulkopuolella.

Yhteiset tutkintaryhmät (Joint investigation team)

Suoranainen operatiivinen yhteistyö on nykyään entistä helpompaa ja tehokkaampaa. Kahden tai useamman EU-maan esitutkintaviranomaiset voivat muodostaa yhteisen tutkintaryhmän toimimaan useamman valtion alueella. Tutkintaryhmän perustaminen on tarpeen, kun tutkittavana on

vakava rikos, jolla on yhteyksiä vähintään kahteen jäsenvaltioon ja rikoksen selvittäminen on vaativaa, tai, kun useat valtiot suorittavat samanaikaisesti esitutkintaa, joka edellyttää useiden maiden välistä koordinoitua ja yhteistä toimintaa.

Yhteisten tutkintaryhmien tutkittaviksi tulevat rikokset ovat usein huumausaineisiin tai ihmis-kauppaan liittyviä rikoksia eli nimenomaan tietoverkkoja hyödyntävää rikollisuutta. Parhailleenkin Suomi on mukana useassa tiimissä.

Interpol

Euroopan ulkopuolelle suuntautuvassa rikostutkinnassa voidaan EU-yhteistyön työkaluja käyttää jossain määrin hyväksi. Pääasiassa turvaudutaan kuitenkin kansainvälisen rikospoliisijärjestön Interpolin palveluihin. Suomen poliisi on osallistunut Interpolin tietotekniikkarikostyöryhmän työskentelyyn aktiivisesti jo vuodesta 1991 lukien.

Pohjoismainen yhteistyö

Verkkorikollisuus on yksi yhteispohjoismaisen rikostorjunnan painopistealueista. Esimerkkinä siitä Suomen, Ruotsin, Norjan ja Tanskan poliisit tekivät kesäkuussa 2009 yhteisiskun, jonka kohteena oli lasten seksuaalista hyväksikäyttöä esittävän kuvamateriaalin hallussapidosta ja levittämisestä epäiltyjä henkilöitä. Yhteisoperaatio toteutettiin eri puolilla Pohjoismaita kaikkiaan 81 eri osoitteeseen. Suomessa kohteita oli 23 ja ne sijaitsivat 14 eri paikkakunnalla. Operaation aikana otettiin kiinni useita epäiltyjä ja takavarikoitiin runsaasti tietokoneita. Iskun perustana oli yhteispohjoismainen projekti, jossa kerättiin yksilöiviä tietoja vertaisverkkojen kautta laitonta kuvamateriaalia ladanneista ja levittäneistä henkilöistä. Suomen tapauksista yksityiskohtana mainittakoon, että eräiden tietokoneiden kovalevyiltä on takavarikoitu noin 8,2 teratavua materiaalia, joka esitutkinnan aikana joudutaan käymään läpi.

Muu yhteistyö

Viranomaisten lisäksi tietoverkossa tapahtuvaa laitonta toimintaa monitoroidaan laajasti ja aktiivisesti ympäri maailmaa myös yksityisellä sektorilla. Tämän vuoksi esitutkintaviranomaiset tekevät tiivistä yhteistyötä tietoturvaviranomaisten lisäksi tietoturvateollisuuden, teleyritysten sekä erityisten tietoturvayhteisöjen kanssa.

LOPUKSI

Tietoverkkorikollisuus täyttää ja nykyisellään menestyksellisen liiketoiminnan vaatimukset. Sangen vaatimattomallakin panoksella voidaan hankkia suurta hyötyä. Toistaiseksi meitä suomalaisia on suojannut massiiviselta tietoverkkorikollisuudelta erikoinen kieli sekä hyvä valmius käyttää tietoturvatyökaluja ja noudattaa tietoturvakäytänteitä.

Olemme kuitenkin maapalloistumassa huimaa vauhtia, eivätkä edellispäivän lainalaisuudet enää välttämättä päde huomispäivän todellisuudessa. Tietoverkko ja sille rakennettu palvelu on ottamassa elämänmenossa alati suuremman roolin. Julkisen ja yksityisen sektorin palvelut, yksityishenkilöt ja yhteisöt, lähes koko infrastruktuuri, tukeutuu tavalla tai toisella tietoverkkoon.

Lainsäädäntö muokkautuu kehityksen ja kokemuksen myötä. Nykyiset esitutkinta- ja syyttäjäviranomaisten käytössä olevat keinot on suunniteltu lähtökohtaisesti perinteisempään käyttöön. Viranomaisten käytössä olevaa keinovalikoimaa ei ole ”tuunattu” tietoverkon nopeuksiin, massiivisiin vaikutuksiin sekä maantieteellisiä rajoja ylittävään toimintaan.

Verkon kehitystä ja sen yhteiskunnallista merkitystä tarkastellessa on jo puute sekin, ettei käyttäjien suojaamiseksi ole jo omaa lukua pakkokeinolaissa. Tällä haavaa tietoverkkoa koskeva säännöstö pohjautuu teletoimintaan, vaikka tieto- ja televerkot ovat jo perusfilosofialtaan hyvin erilaisia.

Tiedon välittäminen verkossa tuntuu olevan erityissuojeltua verrattuna perinteiseen tiedonvälitykseen. Suojeluaspekti tulisikin nykyistä paremmin huomioida myös uhrin kannalta. Tietoverkko toimii postiliikenteeseen rinnastettavan filosofian mukaisesti. Tällä hetkellä viranomaiset voivat puuttua ”haitalliseen” postilähetystykseen seuraavasti:

- tavallisen postikirjeen voi takavarikoida, jos tapauksessa on syytä epäillä rikosta, josta on säädetty vähintään vuosi vankeutta
- sähköpostiviestiin kohdistettava vastaava toimenpide voidaan suorittaa, mikäli tapauksessa on syytä epäillä rikosta, josta on säädetty vähintään neljä vuotta vankeutta

Rikolliseen toimintaan viittaaviin valmistelutoimenpiteisiin tulisi voida pystyä puuttumaan nykyistä aikaisemmassa vaiheessa - eikä vasta sitten, kun asianomistajajoukko koostuu useista tuhansista henkilöistä, mahdollisesti useissa eri valtioissa, tai kun vahingot ovat jo ehtineet miljoonaluokkaan.

Bitti-ilmastoa ajatellessa tulee eittämättä mieleen, että olemme vasta tutustumisvaiheessa verkkomaailmaan ja sen tarjoamiin lähes rajattomilta tuntuviin elämää helpottaviin mahdollisuuksiin. Tietoverkkomaailman tarjoamista hyödyistä emme kukaan tietenkään tahdo luopua tulevaisuudessakaan, vaikka tekninen kehitys - kuten yleensä aina - tuokin mukanaan mahdollisuuksia myös negatiivisille ilmiöille. Valtaosa väärinkäytöksistä on kaiken lisäksi estettävissä käyttäjien omin, varsin yksinkertaisin toimenpitein. Uhkia on runsaasti, mutta niin on torjuntakeinojakin. Totuttelun myötä oppinemme käyttämään ja käyttäytymään yhä tärkeämmäksi käytävässä verkkomaailmassa kuten arkielämässä kotoa kauppaan mentäessä konsanaan. Auton ovet lukitaan ja lompakko pidetään taskussa napin takana maksamiseen asti. Verkkorikollisuuden torjunta on kaikessa yksinkertaisuudessaan vain tilanteen mukaista kohtuullista huolellisuutta ja terveen järjen käyttöä.