POLIISIN ROOLI VERKOSSA VÄKIVALTAISEN EKSTREMISMIN EHKÄISYSSÄ JA SIIHEN VASTAAMISESSA (PVE ja CVE)

Tarvitaan verkosto ekstremistisen verkoston kukistamiseen
EX-POST PAPER
The role of police online in PVE and CVE
Oslo, Norway
April 2018

Online-maailmaa ei voida jättää ekstremistisille verkostoille. Poliisi toimii hyvin aktiivisesti ekstremismin torjumiseksi, mutta tätä toimintaa tulee laajentaa myös online-maailmaan, verkkoon (1). Sosiaalinen media toimii ekstremistien vahvuutena. Tästä syystä poliisi ei voi jättää verkkoa valvomatta. On olemassa monia syitä, minkä takia poliisin tulisi olla läsnä verkossa. Vaikka niin sanottu kalifaatti on saattanut menettää alueitaan, ekstremistisiä jihadistisia ideoita pidetään elossa verkossa. Verkko-jihadismi tukee fyysistä jihadismia. Daesh ja Al-Qaida käyttävät internetiä ideoidensa propagoimiseen sekä terroristisen viestiensä levittämiseen, tavoitteenaan polarisoida yhteisöjä sekä mobilisoida, värvätä ja radikalisoida tukijoita (2).

Jihadistiset verkostot eivät ole ainoita, jotka osaavat käyttää sosiaalista mediaa hyväkseen. Myös äärioikeistolaiset tekevät niin. Äärioikeistolaisilla ryhmillä on omia sosiaalisen median areenoita ekstremistisille ideologioille sekä vihaisille ja haavoittuvaisille yksilöille. Näillä areenoilla muokataan tietoa sekä luodaan informaatiokuplia, joiden avulla voidaan levittää valeuutisia ja muuta propagandaa. Internet tarjoaa yksilöille ja ryhmille mahdollisuuden luoda samoin ajattelevien verkostoja, joissa voidaan inspiroida ja kouluttaa muita (2).

Terrori-iskuja toteuttavat myös yksittäiset toimijat. Vaikka he saattaisivatkin toimia yksin, ovat nämä yksilöt yleensä sulautuneet ekstremistiseen verkostoon. Internetillä onkin suuri rooli radikalisoitumisessa. Jotkut yksittäiset toimijat toteuttavat hirmutekojaan ohjeiden mukaan, mutta toiset ovat yksinkertaisesti inspiroituneita ja toimivat enemmän tai vähemmän yksin. Tämä johtajaton vastarinta syntyy verkkoilmapiirissä, jossa yksittäisiä toimijoita kutsutaan toimimaan. Yksilöt voivat löytää verkosta ehdotuksia siihen, ketä valita iskujen kohteiksi tai kuinka toteuttaa iskuja (2).

Internetin valvominen
IRU (Internet Referral Units) on keskeinen osa poliisien suorittamaa verkkovalvontaa. IRU keskittyy kahteen tärkeään verkkopropagandan osa-alueeseen: viesteihin ja niiden jakamiseen. On tärkeää valvoa, ymmärtää ja toimia. Valvonta on erityisen tärkeää, sillä sen avulla pysytään kärryillä siitä, mitä terroristit tekevät verkossa. Tämä taas auttaa poliisia ymmärtämään, mitä tapahtuu internetissä ja mitä saattaa tapahtua oikeassa maailmassa jossain vaiheessa (3).

Ymmärtääkseen ja tunnistaakseen verkossa olevia ekstremistejä ja terroristisia sisältöjä, IRU käyttää puoliautomaattisia järjestelmiä ja ihmisten tekemää arviointia. IRU käyttää työkaluinaan ohjelmia, jotka skannaavat ja arvioivat verkostoja, käyttäjiä ja sisältöä – tämä onkin merkittävä osa väkivaltaisen ekstremismin ehkäisyä ja siihen vastaamista verkossa. On lisäksi tärkeää pysyä mukana internetin kompleksisuudessa, sekä käytettyjen areenoiden ja teknologioiden kehityksessä. Teknologia ei voi kuitenkaan tehdä kaikkea yksin, vaan tarvitaan myös ihmisälyä ja ihmisen tekemää arviointia. Havaitessaan ekstremistisiä viestejä tai yksilöitä, IRU aloittaa tutkinnan tai ottaa yhteyttä palvelun tarjoajaan, pyytäen tätä poistamaan kyseessä olevan kohteen tai sulkemaan tilin. Verkossa tapahtuva PCVE-toiminta edellyttääkin yhteistyötä internet-teollisuuden kanssa (3).

Online-offline välisen aukon yhteen kurominen
Online- ja offline-maailmoiden välillä tapahtuu jatkuvaa vuorovaikutusta. IRU toimii kahdenlaisten joukkojen kautta. Yksi joukoista keskittyy internetin valvontaa ja tutkimiseen, varmistaen, että toimenpiteitä otetaan käyttöön, kun jotakin löytyy. Toiminta voi olla kiireellistä, jos uhka on välitöntä tai se voi olla kohteen poistamista, tutkintaa tai syytteen nostamista. Työtä tehdäänkin niin, että internet-tapauksia voidaan asettaa syytteeseen. Toinen joukoista keskittyy vastamaan poliisien tukipyyntöihin, joissa tarvitaan asiantuntijuutta, informaatiota tai muuta apua esimerkiksi tilanteissa, joissa epäillyn digitaalista toimintaa täytyy ymmärtää paremmin (3).

Norjalla on omanlaisensa tapa kuroa yhteen poliisien online- ja offline-työtä. NCIS (The National Criminal Investigation Service) on perustanut verkkoon useita areenoita, joiden kautta poliisi voi olla läsnä. Lisäksi se on perustanut cyber-partion Facebookiin: poliisilla on oma Facebook-sivunsa ja Facebook-profiilinsa. Poliisin Facebook-sivu on koko ajan käytössä, profiili sen sijaan yhä testauksessa. Facebook-sivun kautta poliisi on läsnä ja tekemisissä ihmisten kanssa monin eri tavoin. Facebook-sivu toimii poliisin ehkäisevänä linnakkeena, ja sitä voidaankin verrata konkreettiseen poliisiasemaan, jossa ihmiset voivat ottaa yhteyttä poliisiin. Sivulla on kaksi päätehtävää:

1) Vastata kysymyksiin sekä arvioida vihjeitä, joita ihmiset ovat lähettäneet
2) Julkaista postauksia ja sisältöä eri aiheista, kuten väkivaltaisen ekstremismin ehkäisystä sekä ohjeistuksia nuorille, vanhemmille ja aikuisille

Facebook-sivu tavoittaa tuhansia ihmisiä. Projektin päätavoitteena on luoda toimintatapoja ja ohjeita ehkäisevää työtä tekeville poliiseille (3). Kaikki Norjan 12 poliisialuetta ottavat käyttöön internet-poliisin vuonna 2018. Facebook-profiili tulee toimimaan operationaalisena poliisipartiona verkossa, tehtävänään taistella väkivaltaista ekstremismiä ja radikalisoitumista vastaan. Tavoitteena on lisätä tietoisuutta rikollisesta ja huolestuttavasta käytöksestä suljetuissa ryhmissä sekä kannustaa sivustojen ja ryhmien ylläpitäjiä poistamaan laitonta materiaalia (4).

Tarve ymmärtää: strateginen analyysi ja strateginen kommunikointi
Interpolin ja poliisin tavoitteena on kuroa yhteen ehkäisevä työ ja tutkinta. Huomaaminen ja toiminta ovat poliisin internet-toiminnan keskiössä. Toiminnan ja huomaamisen lisäksi on tärkeää pyrkiä analysoimaan ja ymmärtämään, miten verkko kehittyy. Ekstremistien tavat käyttää viestejä ovat kehittyneet aikojen saatossa, samoin myös teknologiat, joiden kautta ekstremistit levittävät viestejään. Poliisin tulee olla tietoinen näistä muutoksista ja yrittää pysyä mukana niissä – mieluusti jopa askeleen tai kaksi ekstremistien edellä. Verkossa tapahtuvan kehityksen ymmärtäminen tarkoittaa, että ymmärretään viesteissä ja niiden levittämisessä tapahtuvat muutokset (4).

Radikalisoituneiden yksilöiden takavarikoiduista puhelimista ja tietokoneista löytyy pääosin väkivallatonta sisältöä, sisältäen Daeshin propagandaa veljeydestä, yhteenkuuluvuudesta ja mahdollisuuksista kalifaatissa. Teloittamisen sijaan ihmisiä kiehtookin yhteenkuuluvuuden tunne, ja tämä tieto voidaankin ottaa huomioon, kun mietitään, minkälainen internet sisältö vaikuttaa radikalisoitumiseen. Tämä tieto on tärkeää ehkäisevän toiminnan kannalta, kuten vaihtoehtoisten viestien ja radikalisoitumiseen vastaavien viestien suunnittelussa (4).

Radikalisoituminen voidaan nähdä kommunikoinnin ongelmana. Ihmiset uskovat jihadistista ja muuta propagandaa, koska heidän käsityksensä maailmasta ja heidän roolistaan siinä on tietynlainen. Kommunikoinnin kautta voidaan muuttaa tätä käsitystä todellisuudesta (4).

- Esimerkki: Väestöllä voi olla vaihtelevia näkemyksiä. Vasemmalla ovat ihmiset, jotka ovat sitä mieltä, että ihminen voi olla samaan aikaan britti ja muslimi. Oikealla olevat ihmiset taas uskovat vahvasti Daeshin propagandaan, että ihmisen tulee valita vain toinen näistä, et-

kä voi yhdistää näitä kahta: olet joko Daeshin puolella tai sitä vastaan, joko oikea muslimi tai et. Tämän puolen ihmiset ovat alttiita radikalisoitumiselle ja värväämiselle. Vasemman ja oikean sivun keskelle jäävät ihmiset, jotka joskus painivat näiden kahden identiteetin yhdistämisen kanssa (4-5).

Propagandan, vihapuheen sekä muun negatiivisen ja ihmisiä jakavien viestien ongelmana on, että ne työntävät kohdeyleisöään oikealle sivulle. Tästä syystä tuleekin vastata, häiritä ja poistaa viestejä, jotka työntävät ihmisiä väärään suuntaan. Samaan aikaan tulee myös luoda vaihtoehtoisia ja positiivisia viestejä. jotka edesauttavat ihmisten siirtymistä vasemmalle puolelle (5).

Verkko-vastustuskykyyn investoiminen= rikoksien ehkäisyä

Emme pysty koskaan poistamaan kaikkea ekstremististä sisältöä internetistä tai blokkaamaan jakamista vertaisten kesken, oli sisältö salakoodattua tai ei, avoimilla foorumeilla tai suljetuissa foorumeissa olevaa. Jotain sisältöä on vaikea todistaa laittomaksi tai radikalisoivaksi, vaikka radikalisoituneet toimijat käyttäisivät sitä ekstremismiin kannustavana tai ohjaavana. Lisäksi demokraattisiin arvoihin kuuluvan sananvapauden vuoksi internetissä tulee aina olemaan kiistanalaista materiaalia, joka tulisi osan mielestä poistaa. Lyhyesti: internetissä tulee aina olemaan ekstremististä sisältöä, lyhyemmän tai pidemmän ajan.

Tästä syystä ekstremistiseen sisältöön ja viesteihin keskittymisen sijaan on tärkeää työskennellä viestien vastaanottajien parissa. Yhteiskunnasta ja alttiista yksilöistä tulee tehdä vastustuskykyisiä. Tämä on yksi tapa ehkäistä rikoksia. Medialukutaito ja verkkoturvallisuus ovat alueita, joilla poliisi voi saada aikaan tuloksia nuorten, heidän vanhempiensa ja opettajiensa kanssa. Propagandan, valeuutisten ja salaliittoteorioiden tunnistaminen ovat uusia taitoja, joita nuorten on nykyisin hyvä osata (5).

Taistelu vihapuhetta vastaan ja vastustuskyvyn lisääminen

”Vihapuhe kattaa kaikki ne ilmaisun muodot, jotka levittävät, kannustavat, edistävät tai oikeuttavat rotuun liittyvän vihamielisyyden, muukalaispelon, antisemitismin ja muut vihamielisyyteen perustuvat suvaitsemattomuudet” (Euroopan neuvoston määritelmä) (5).

Vihapuheen vastaisen työn tukeminen tai toimeenpaneminen ovat rikoksien ehkäisyä. Saksassa on toimeenpantu vihapuhe-projekti ”Helden statt Trolle”, ja sen tarkoituksena on herkistää poliisi ja yhteiskunta vihapuheelle ja valeuutisille kehittämällä ja kouluttamalla ihmisiä vastareaktioihin. Projekti toimii online- ja offline-ympäristöissä ja tukee näin ollen online- ja offline-yhteisöjä vihaa vastaan (5). Vihapuheeseen vastaaminen ja sen vastainen taistelu tukevat niitä tekijöitä, jotka työntävät ihmisiä haluttuun suuntaan: vasemmalle. Tarvitaan vähemmän propagandaa jakavia viestejä sekä enemmän vaihtoehtoisia ja positiivisia viestejä. Vihapuheen vastaiset kampanjat voivat mobilisoida sosiaalista vastustuskykyä ja johtaa tilanteeseen, jossa vihapuhetta poistetaan entistä enemmän verkosta. Kampanjoilla on puhdistava vaikutus niihin kasvualustoihin, joilla radikalisoituneet värvääjät toimivat (6).

Työskentely kansalaisjärjestöjen kanssa

Vihapuheen vastaiset kampanjat ovat esimerkkejä kansalaisjärjestöjen ja poliisin välisestä yhteistyöstä. Esimerkiksi saksalainen kansalaisjärjestö ”Jugendschutz.net” pyrkii suojelemaan nuoria vahingoittavalta sisällöltä. Tämä laaja määritelmä takaa, että lainmukaisilla toimijoilla on enemmän mahdollisuuksia tehdä interventioita. Jugendschutz voi toimia kaikkea sellaista sisältöä vastaan, jonka se ymmärtää nuorille haitalliseksi. Kansalaisjärjestö perustettiin vuonna 2011 vastaamaan äärioikeiston ekstremismiin, jihadismi astui mukaan myöhemmin. Se keskittyy yleiseen valvontaan sekä keskitetympään tutkimiseen. Yksilöt voivat myös osoittaa järjestölle sisältöä, ja järjestö onnis-

tuu 90% varmuudella poistamaan haitallisena pidetyn kohteen. Järjestö ja poliisi pitävät toisensa ajan tasalla. Järjestö työskentelee sellaisen sisällön kanssa, johon poliisilla ei ole joko aikaa tai oikeutta puuttua (6).

Poliisit verkossa: kommunikointityylit
Pelkkä verkossa läsnä oleminen ei riitä, jos poliisit tahtovat olla tekemisissä ihmisten kanssa (6). Huumorin ja kiinnostavien kuvien käyttäminen voivat lisätä onnistunutta verkkokommunikointia sekä lisätä huomiota. Viestien tulisi myös vedota tunteisiin sekä näyttäytyä paikkansapitävinä yleisölle (6-7).

Internet-teollisuus ja yhteistyöverkosto
Ekstremistit ovat taitavia verkostoitumaan ja käyttämään verkostoja rikollisiin tarkoituksiinsa. Sitoutuneet tukijat auttavat jakamaan viestejä ”suljettuihin alueisiin”, joissa on paljon tukijoita. Jotta poliisi voi toimia tehokkaasti ekstremistien verkostoja vastaan, tulee sen muodostaa oma verkostonsa. Kansalaisjärjestön ja koulutussektorin saralta poliisi voi löytää partnereita, jotka tunnistavat haitallista sisältöä ja edesauttavat niiden poistamista. Internet-teollisuudella on myös oman alansa kokemusta sekä mahdollisuus päästä käsiksi käyttäjiin. Poliisin ja hallituksen tuleekin kannustaa internet-teollisuutta ottamaan vastuuta asian tiimoilta. Internet-teollisuuden vastuulla on taata, että sen tarjoama ympäristö ei edistä ekstremismiä tai terrori-iskujen tekemistä, ja ettei sen ympäristöjä käytetä terroristisen materiaalin julkaisemiseen ja jakamiseen.

- Esimerkki Facebook: Facebookilla on oma väkivaltaisen ekstremismin vastainen joukko, joka koostuu eri taustoista tulevista ammattilaisista, kuten kansalaisjärjestöistä, poliisista ja hallinnollisista edustajista. Facebook yrittää poistaa sivuiltaan ekstremististä ja häijyä sisältöä. Se pystyy merkitsemään ladattua sisältöä ja luomaan sille digitaalisen sormenjäljen. Jos sama sisältö ladataan uudestaan, kone tunnistaa ja poistaa sen nopeasti (7)

Yhteistyö internetin palveluntuottajien voi tehdä suuren eron toimintaan (8).