MAANPUOLUSTUSKORKEAKOULU

AUTOMATISOIDUT RAJATARKASTUKSET

Pro Gradu -tutkielma

Kadetti
Tommi Tiilikainen

Kadettikurssi 92
Rajavartiolinja

Maaliskuu 2009

MAANPUOLUSTUSKORKEAKOULU

Kurssi Kadettikurssi 92	Linja Rajavartiolinja
Tekijä Kadetti Tommi Tiilikainen	
Pro Gradun nimi **Automatisoidut rajatarkastukset**	
Oppiaine, johon työ liittyy Tekniikka	Säilytyspaikka Kurssikirjasto (MpKK:n ja RMVK:n kurssikirjastot)
Aika: maaliskuu 2009	Tekstisivuja 56 Liitesivuja 0

TIIVISTELMÄ

Tutkimuksessa ”Automatisoidut rajatarkastukset” selvitetään mitä automatisoidut rajatarkastukset tarkoittaa, mihin se perustuu, mikä se on ja miksi siihen halutaan siirtyä. Tutkimuksessa automatisoiduilla rajatarkastuksilla ei tarkoiteta pelkästään passin tarkastavaa automaattista porttia, vaan laajemmin rajatarkastustekniikan muuttumista automaattisemmaksi.

Tutkimuksessa selvennetään rajaturvallisuutta yleisesti. Pääpaino tutkimuksessa on automatisoitujen rajatarkastusten kokonaisuuden selvittämisessä. Suomessa Automatisoidut rajatarkastukset ovat vielä suunnittelu-, kehittely- ja kokeiluasteella. Yhdysvalloissa on Smart Border -niminen rajatarkastusmalli jo käytössä jossain määrin. Myös muualla maailmalla on kokeilukäytössä erilaisia automaattisia rajatarkastuslaitteita.

Automatisoiduilla rajatarkastuksilla halutaan vastata tämän päivän haasteisiin rajaturvallisuutta vastaan. Automatisoiduissa rajatarkastuksissa käytetään tämän hetkistä huipputekniikkaa. Tekniikka onkin yksi automatisoitujen rajatarkastusten peruspilareista.

Smart Borderin tavoitteena on rajankulun parantaminen ja peruspilarit siihen ovat: seulonta, biometriikka ja informaatioteknologia. Näillä työkaluilla paranee niin rajaturvallisuus, kuin valtion sisäinenkin yleinen järjestys ja turvallisuus.

Tutkimus on tehty perehtymällä erilaisiin lähdemateriaaleihin Smart Borderin periaatteista, biometriikasta sekä Suomen automatisoitujen rajatarkastusten kehittämissuunnitelmista. Tutkimuksessa on ollut haasteellista aiheen tuoreus. Suomen automatisoituja rajatarkastuksia koskien lähdemateriaalia on ollut vain vähän saatavilla johtuen kehittely- ja kokeiluvaiheesta, eikä aiheesta ei ole vielä tehty muita tutkimuksia. Yhdysvaltojen Smart Borderista, biometriikan soveltuvuudesta rajaturvallisuuteen sekä automatisoinnista yleisellä tasolla on ollut enemmän materiaalia saatavilla. Lisäksi haasteena on aiheen nopea kehittyminen. Muutoksia tapahtuu nopeasti ja tutkimuksen kolmevuotisen elinkaaren ajalle mahtuu paljon muuttuvia asioita.

AVAINSANAT
Rajaturvallisuus, automatisoidut, rajatarkastukset, smart border, biometriikka, passiautomaatti

AUTOMATISOIDUT RAJATARKASTUKSET

AUTOMATISOIDUT RAJATARKASTUKSET

1. JOHDANTO

Tämän tutkimuksen aiheena on automatisoidut rajatarkastukset. Tässä tutkimuksessa käsitellään mitä automatisoiduilla rajatarkastuksilla tarkoitetaan pelkän automaattisen passintarkastusportin lisäksi. Tässä tutkimuksessa on tarkoitus myös selvittää mihin automatisoidut rajatarkastukset perustuvat, miten ne toimivat ja mitä etuja niillä on tarkoitus saavuttaa. Tässä yhteydessä tulee selvitetyksi, mitä uutta automatisoidut rajatarkastukset tuovat sekä Rajavartiolaitokselle että yhteiskunnallekin nykyisten voimassaolevien rajatarkastusten sijaan, lisäksi tai tueksi. Mikä voisi olla ratkaisevin peruste siirtyä nykyisten rajatarkastusmenetelmien sijaan suorittamaan rajatarkastukset automatiikkaa hyödyntäen.

Automatisoituja rajatarkastuksia on ollut kehitteillä jo useita vuosia ja kehitys jatkuu koko ajan. Varsinainen lähtölaukaus kehittelylle oli kuitenkin Yhdysvalloissa tapahtunut tuhoisa syyskuun 11. päivän terrori-isku vuonna 2001. Tässä koko maailmaa pysäyttäneessä tragediassa terroristiryhmä pääsi yllättämään yhdysvaltalaisten metropoliittojen arkipäivän täydellisesti jättäen jälkeensä suunnatonta tuskaa, surua, pelkoa ja vihaa. Tämä oli Yhdysvalloissa käännekohta tavoitella varmempia menetelmiä taata kansalaisten turvallisuus sekä poliittisesti että yhteiskunnallisesti. Koska ei ole ollut olemassa mitään kansainvälisesti sovittua virallista tai edes yhtenäistä mallia automatisoiduille rajatarkastuksille, on jokainen valtio alkanut soveltaa itselleen omaan yhteiskuntaansa ja kulttuuriinsa sopivinta mallia. Automatisoitujen rajatarkastusten kehittelyn lähtökohtana on ollut juuri rajaturvallisuuden parantaminen. Samalla, kun rajaturvallisuutta on haluttu parantaa, on pyritty pitämään mielessä samanaikaisesti niin sanottujen tavallisten rajan ylittäjien kuin myös yhteiskunnalle ja taloudelle tärkeiden tuonti- ja vientitavaroiden sujuva ja vaivaton liikkuminen eri valtioiden välillä.

Rajaturvallisuuden parantaminen tämän tutkimuksen kirjoittamisen aikoihin tarkoittaa käytännössä tiukempia rajatarkastuksia. Tiukemmat rajatarkastukset puolestaan tarkoittavat ihmisten ja ajoneuvojen manuaalista tarkastamista eli rajavartiomiehen

henkilökohtaisesti tekemää tarkastusta. Luonnollisesti tämä on aikaa vievää, joka voi helposti aiheuttaa ruuhkia rajanylityspaikoille rajavartiomiehen tutkiessa matkustusasiakirjojen aitoutta ja maahantuloedellytyksiä. Odotusajat voivat pahimpien ruuhkien aikaan venyä tavallisten matkustajien osalta jopa useisiin tunteihin ja rekkaliikenteen osalta jopa kymmeniin tunteihin. Kaakkois-Suomen useiden vuorokausien rekkajonot rajalle vievien teiden varsilla eivät kuitenkaan johdu pelkästään rajatarkastuksista. Teollisuudelle tärkeitä tuontitavaroita ei kuitenkaan ole taloudellisesti järkevää seisottaa rajalla odottamassa pääsyä maahan ja tehtaan linjastolle.

Rajatarkastusten tehostamisen jälkeen Yhdysvalloissa huomattiin, ettei nykyisessä globalisaatio-yhteiskunnassa voi turvallisuuden lisäämisen perusteella yksinkertaisesti vain sulkea rajoja ja eristäytyä muulta maailmalta. Yhdysvallathan lähes sulkivat rajansa syyskuun 11. päivän terrori-iskujen jälkeen, ja aloittivat äärimmäisyyksiin asti viedyt rajatarkastukset. Tiukentuneet rajatarkastukset aiheuttivat luonnollisesti odotusaikojen pidentymistä raja-asemilla muutamasta minuutista yli kymmeneen tuntiin[3]. Tuontitavaroiden odotusajat puolestaan kasvoivat rajalla niin merkittävästi, että näistä viivytyksistä johtuneet tavaroiden toimitusaikojen myöhästymiset, aiheuttivat jopa miljardien dollareiden tappiot teollisuudelle. Esimerkiksi Fordin autotehdas joutui jopa sulkemaan tehtaitaan Michiganissa sekä Windsorissa johtuen rajatarkastusten aiheuttamista toimitusaikojen pidentymisestä [3]. Tiukentuneiden rajatarkastusten kohteeksi joutuivat myös lomamatkailijat. Tuntien jonotusajat rajalla sai ihmiset perumaan tai siirtämään lomamatkojaan, josta puolestaan oli seurauksena merkittäviä taloudellisia vaikutuksia matkojen järjestäjien kannattavuuteen.

Tarvitaan siis selkeä ja luotettava menetelmä, mikä estää terroristien sekä rikollisten maahantulon, mutta samanaikaisesti mahdollistaa niin ihmisen, tavaran kuin pääomankin vapaan ja sujuvan liikkumisen rajan yli. Tämän yhtälön ratkaisemiseen haetaan vastausta automatisoiduista rajatarkastuksista.

Yhdysvalloissa rajaturvallisuuden parantamista on tutkittu paljon syyskuun 11. päivän World Trade Centeriin kohdistuneiden terrori-iskujen jälkeen. Suomessa automatisoidut rajatarkastukset ovat vasta kehittely-, suunnittelu-, ja kokeiluasteella. Tästä johtuen tämä tutkimus pohjautuukin pitkälti teorian osalta Yhdysvaltalaiseen Smart Border –ajatukseen. Käytännöstä kertova osa perustuu yleisiin tällä hetkellä maailmalla oleviin automatisointeihin ja tulevaisuuden näkymiin. Yhdysvallat ovat tehneet jo käytännön kokeiluja Smart Borderiin liittyen ja se on jossain määrin jo

käytössäkin Yhdysvalloissa. Smart Border ei kuitenkaan ole ainoa laatuaan maailmassa, eikä se ole mikään erillinen laite vaan eräänlainen viitekehys automatisoiduille rajatarkastuksille. Maailmalla on erilaisia automatisointeja rajatarkastuksiin liittyen kokeilukäytössä. Kaikki ne perustuvat suuressa mittakaavassa Smart Border – ajatuksen viitekehykseen, laitteistot saattavat vaihdella huomattavasti maiden välillä. Suomessakin Helsinki-Vantaan lentoasemalla on tällä hetkellä kokeilukäytössä Portugalista tullut Vision-Box:in valmistama VBeGate -merkkinen automaattinen passintarkastusportti.

Smart Border on se työkalu, jolla vastataan uhkakuviin rajaturvallisuutta vastaan. Smart Border hyödyntää uusinta teknologiaa, mikä osaltaan mahdollistaa rajatarkastusten parantamisen. Kehittyneen teknologian myötä kolmeksi tärkeimmäksi Smart Border -ajatuksen peruspilariksi onkin muodostunut seulonta, biometriikka ja informaatioteknologia. Smart Borderista kerrotaan enemmän kappaleessa 3.

1.1 TUTKIMUSASETELMA

1.1.1 Tutkimusaiheen valinta

Tutkimuksen aiheen valintaan vaikutti Antti Eskolan ajatus, että ”tutkijan tulisi suuntautua itseään kiinnostaviin tutkimusaiheisiin, koska silloin hän voisi parhaalla mahdollisella tavalla käyttää innostuksensa, tietonsa ja oivalluskykynsä hyödykseen huolimatta siitä, kohdistuvatko nämä voimavarat todella tärkeiden ongelmien selvittelyyn. Tärkeintä on sallia jokaisen tutkijan toimia omien intressiensä suuntaisesti rajoittamatta heidän vapauttaan minkään yhteisen suunnitelman nimissä” [6].

Tämän oivallettuani, ja saatuani tietoon valittavissa olevat tutkimusaiheet oli oman tutkimukseni aihevalinta saman tien selvä. Automatisoidut rajatarkastukset ovat niin ajankohtainen asia, että vasta viime kesänä (8.7.2008) Helsinki-Vantaan lentoasema sai koekäyttöön ensimmäiset automaattiset rajatarkastusportit. Automatisoidut rajatarkastukset ovat toki muutakin kuin pelkkä portti lentoasemalla, mutta portit ovat sen näkyvin osa. Automatisoidut rajatarkastukset koskettavat koko Schengen-aluetta.

Automatisoitujen rajatarkastusten ajankohtaisuus, sekä myös niiden tuntuminen oikeasti tärkeältä ja mielenkiintoiselta asialta minulle sai minut lopulta valitsemaan tämän aiheen.

1.1.2 Tutkimusongelman määrittely

Syyskuun 11. päivän 2001 terrori-iskut World Trade Centeriin ja Pentagoniin toimivat lähtölaukauksena automatisoitujen rajatarkastusten kehittämiselle niin Yhdysvalloissa kuin muuallakin maailmassa. Kehitys oli toki menossa koko ajan kohti automatisointeja jo määrärahojen supistamisien takia, mutta terrori-iskut nostivat kehitysvauhdin eksponentiaaliseksi. Kuluneen seitsemän vuoden aikana on tapahtunut todella paljon ja teknologia on edennyt suurin harppauksin eteenpäin. On tullut muun muassa biometriset passit ja automaattiset rajatarkastusportit, eikä loppua vielä ole näkyvissä.

Suomen kohdalla automatisoidut rajatarkastukset elävät tällä hetkellä murrosaikaa. Asioista on olemassa monenlaisia suunnitelmia, mutta mitään konkreettista ei varsinaisesti vielä ole käsillä; kehitteillä on paljonkin. Suomessa ainoa konkreettinen asia tällä hetkellä on koekäytössä olevat automaattiset rajatarkastusportit Helsinki-Vantaan lentoasemalla. Koska automatisoidut rajatarkastukset ovat maailmanlaajuinen asia, ja erityisesti Schengen alueelle yhteinen ja tärkeä asia, on kehityksen seuraaminen haastavaa ja mielenkiintoista. Suurin osa saatavasta materiaalista on tällä hetkellä englanninkielistä, eikä välttämättä kosketa Suomea kuin yleisperiaatteellisella tasolla. Saatavilla olevasta materiaalista saa kuitenkin käsityksen, mitä se voisi olla, tai mitä sen pitäisi olla. Selvää kuitenkin on, etteivät automatisoidut rajatarkastukset tule toimimaan siten, kuin niiden optimaalinen tarkoitus olisi, vielä moneen vuoteen.

1.1.3 Tutkimusasetelma ja tutkimuksen tavoitteet

Tavalliselle matkustajalle automatisoidut rajatarkastukset eivät tarkoita juurikaan mitään muuta, kuin uuden kalliimman biometrisen passin hankkimista ja sen uusimista useammin kuin vanhan passin. Biometrisen passin voimassaoloaika on vain viisi vuotta vanhan mallisen passin kymmenen vuoden voimassaolon sijaan. Tavallinen matkustaja pääsee uudella biometrisella passilla automaattisen rajatarkastusportin

läpi näkemättä rajavartijoita lainkaan. Tässä on käytännössä ne muutokset, mitä automatisoidut rajatarkastukset tuovat tavalliselle matkustajalle. Ihmillä on taipumus olla epäluuloinen ja vastaan kaikkea uutta, siksi julkisuudessa on ollut keskustelua myös siitä, että tämä olisi vain hallituksen keino vahtia kansalaisia.

Automatisoidut rajatarkastukset ovat kuitenkin kulissien takana niin paljon kaikkea muutakin, kuin esiin nostettua hallituksen valvontaa ja passintarkastusportteja. Näkökulmaksi olen valinnut tavallisen matkustajan, joka ei vielä tiedä eikä siten ymmärrä perimmäisiä syitä miksi automatisoituihin rajatarkastuksiin siirrytään ja mitä ne yli-päänsä tarkoittavat.

Tutkimuksen ensisijaisena ja realistisena tavoitteena on pyrkiä selvittämään kansantajuisesti mitä kaikkea automatisoidut rajatarkastukset tarkoittavat ja miksi siihen ollaan siirtymässä. Miksi automatisoidut rajatarkastukset ovat parempi menetelmä kuin vanha? Mitä käytännön toimenpiteitä niistä aiheutuu, vai aiheutuuko? Käytän tietoisesti termiä kansantajuisesti, sillä tällaiset huipputeknologiaan liittyvät tekniset asiat muuttuvat helposti vaikeatajuisiksi suuren yleisön pohtiessa näitä asioita keskuudessaan. Ihmiset saattavat jopa jossain määrin tarkoitushakuisesti ymmärtää ne vaikeasti, kun on kyse uudesta tekniikasta. Eivätkä byrokraattiset Euroopan Yhteisöjen komission tiedoksiannot parlamenteille ja neuvostoille ole välttämättä yhtään sen helpompitajuisia, puhumattakaan Eduskunnan Internet-sivujen tiedotuspalvelusta ajankohtaisista asioista. Ymmärtämisen helpottamiseksi olenkin pyrkinyt käyttämään mahdollisimman yksinkertaisia esimerkkejä ja havainnollistavia mielikuvia muun muassa elokuvamaailmasta. Asian ymmärtämisen kannalta on helpompaa, kun saa ”nähdä” mitä se tarkoittaa.

1.1.4 Tutkimuksen viitekehys

Viitekehyksenä tutkimukselle toimii automatisoidut rajatarkastukset. Raamit viitekehykselle antavat rajavartiolain (578/2005), Schengen Borders Code ja EU:n asetusten määräykset rajatarkastuksesta, sekä rajatarkastusten automatisoinneista. Tämä vuoden 2005 syksyllä ilmestynyt uusi rajavartiolaki toi Rajavartiolaitokselle paljon lisää toimivaltaa. Tämän kyseisen lain tarkennettu versio on vuoden 2008 joulukuussa ollut valiokunnan käsittelyssä, mutta ei ole vielä edennyt valmiiksi laiksi asti tämän tutkimuksen kirjoittamisen hetkellä. Tässä laissa, sekä EU:n asetuksissa määrätään muun muassa kuinka rajatarkastuksia saa automatisoida.

1.1.5 Tutkimusstrategian ja tutkimusmenetelmien valinta

Tutkimusstrategialla tarkoitetaan tutkimuksen menetelmiin kohdistuvien ratkaisujen kokonaisuutta ja se perustuu tutkijan yhdenmukaisiin valintoihin [5]. Tutkimuksen tarkoitus ohjaa tutkimuksen strategisia valintoja.

Tutkimusstrategia voi olla

1. kokeellinen, jossa mitataan yhden käsiteltävän muuttujan vaikutusta toiseen muuttujaan,
2. survey-tutkimus, jossa tietoa kerätään standardoidussa muodossa joukolta ihmisiä tai
3. tapaustutkimus (case-study), jossa tutkitaan yksityiskohtaista, intensiivistä tietoa yksittäisestä tapauksesta tai pienestä joukosta toisiinsa suhteessa olevia tapauksia.

Tämä tutkimus on tapaustutkimus automatisoitujen rajatarkastusten (Smart Border –viitekehys) soveltumisesta Suomen olosuhteisiin, lähinnä Helsinki-Vantaan lentoasemalle. Koska tämän tutkimuksen tekohetkellä automaattiset rajatarkastusportit ovat vielä koekäytössä Helsinki-Vantaan lentoasemalla, joudun turvautumaan tässä työssä lähdeaineistoon perustuviin olettamuksiin ja ennustuksiin millaiseksi automatisoitu rajatarkastus todennäköisimmin muodostuu tai millaiseksi sen tulisi muodostua.

Tutkimusstrategiaan liittyy suppeampana käsitteenä tutkimusmetodi eli tutkimusmenetelmä. Tutkimusmenetelmän valintaan vaikuttaa itse tutkimustehtävä ja tutkimuksen luonne: pyritäänkö tieteelliseen vai käytännölliseen tietoon. Automatisoitujen rajatarkastusten tapauksessa on mielestäni tärkeä saavuttaa nimenomaan käytännöllinen tieto kokonaisuuden ymmärrettävyyden parantamiseksi. Tieteellinen näkökulma on toki tärkeää, mutta mikäli pyrittäisiin suoraan tieteelliseen tietoon, niin kokonaisuuden hahmottaminen on mahdollista jäädä lukijalle puutteelliseksi.

Kokeiluasteella olevien automatisoitujen rajatarkastusten tutkimiseen on mielestäni käytettävä eri tutkimusmenetelmiä soveltaen. Tärkeimpänä tutkimusmenetelmänä on niin kutsuttu pöytälaatikko-tutkimus, sillä asian tuoreuden takia tästä aiheesta ei ole aikaisempia tutkimuksia Suomen osalta ja siksi on perehdyttävä suureen määrään erilaista lähdeaineistoa sekä suomalaisista, että ulkomaalaisista lähteistä. Lähteinä

ovat toimineet Smart Border – viitekehyksen teorian osalta Yhdysvaltalaiset lähteet ja varsinaisen automatisoinnin osalta on lähteinä ollut eri valmistajien ja eri maiden rajapalveluiden internet-sivustoja, sekä yleisesti mediassa esillä olleita asioita. Tarkoituksella en ole lähtenyt etsimään Rajavartiolaitoksen esikunnasta suunnitelmia automatisoinneista, jotta tutkimus pysyisi julkisena, eikä menisi salaisen lähdemateriaalin takia turvaluokitelluksi teokseksi. Tukea teorioille saa haastattelemalla niitä henkilöitä, joiden työn tekemiseen automatisoidut rajatarkastukset vaikuttavat suoraan. Tällä hetkellä nämä sellaiset henkilöt työskentelevät Suomenlahden Merivartioston Helsingin Rajatarkastusosastosta Helsinki-Vantaan lentoasemalla. Heidän käytännön kokemuksensa ja siihen perustuva näkemyksensä automaattisten rajatarkastusporttien soveltumisesta käytäntöön on olennainen ja ensiarvoisen tärkeä taustatieto, kun selvitellään automatisoitujen rajatarkastusten soveltumista Suomeen.

1.1.6 Tutkimuksen rakenne ja eteneminen

Koska tätä tutkimusta aloittaessani ei Suomessa vielä ollut edes koekäytössä automaattisia rajatarkastusportteja, aloitan tutkimukseni esittelemällä ensimmäisessä osassa yleisluonnollisesti automatisoitujen rajatarkastusten lähtökohtia ja alan kehityksestä yleisesti. Tuon esille yleiset periaatteet, joita kukin maa on lähtenyt soveltamaan omien tarkoitusperiensä mukaisesti omiin tarkoituksiinsa sopiviksi. Tutkimuksen toisessa osassa tutkin miten automatisoidut rajatarkastukset soveltuisivat Suomeen, ja millainen tämän menetelmän pitäisi olla, jotta sen hyödynnettävyys olisi mahdollisimman tehokas sekä turvallisuuden lisäämisen kannalta että taloudellisesti

1.1.7 Tutkimuksen riskitekijöitä

Jokaisella tutkimuksella on riskitekijänsä. Tutkimuksessa voidaan tutkia kokonaan vääriä asioita, vieraskielisen lähdeaineiston tulkinnassa voi tulla virheellisyyksiä tai vaikkapa haastattelutilanteessa kysymysten muotoilukin voi vaikuttaa kysymysten ymmärtämiseen toisin, kuin on tarkoitettu. On voitu valita väärä tutkimusmenetelmä, tutkijan oma huolimattomuus aineiston ja tulosten käsittelyssä sekä tulkinnassa voi antaa virheellisen kuvan tutkimuksesta. Tutkimus on myös voitu suorittaa ajankohtana, joka poikkeaa liikaa tavanomaisesta.

Tämän tutkimuksen suurimpana riskitekijänä pitäisin sen suoritusajankohtaa. Tutkimuksen tekohetkellä Helsinki-Vantaan lentoasemalla automaattiset rajatarkastuspor-

tit ovat vasta koekäytössä, eikä niistä ole vielä välttämättä saatu tarpeeksi kokemusta kunnollista analysointia varten, puhumattakaan siitä että nämä tiedot olisivat tutkijan käytettävissä. Tällöin on riski, että tutkimuksesta tulee pelkästään teoriapainotteinen ja yksinomaan olettamuksiin ja todennäköisiin mahdollisuuksiin perustuva ”tällainen se voisi tai pitäisi olla” –tyyppinen, eikä niinkään konkreettisesti käytössä olevaa tai tulevaa järjestelmää kuvaava selvitys.

Toinen riskitekijä tälle tutkimukselle on alan nopea kehittyminen. Tieto vanhenee nopeasti ja uusia laitteita ja järjestelmiä tulee koko ajan lisää vauhdilla. Myös Schengen-alue on muuttunut uusien jäsenmaiden myötä kaksi kertaa tutkimuksen aloittamisen jälkeen. Kun tutkimukselle saadaan painettua viimeinen piste, on sisältö saattanut vaihtua jo olennaisesti.

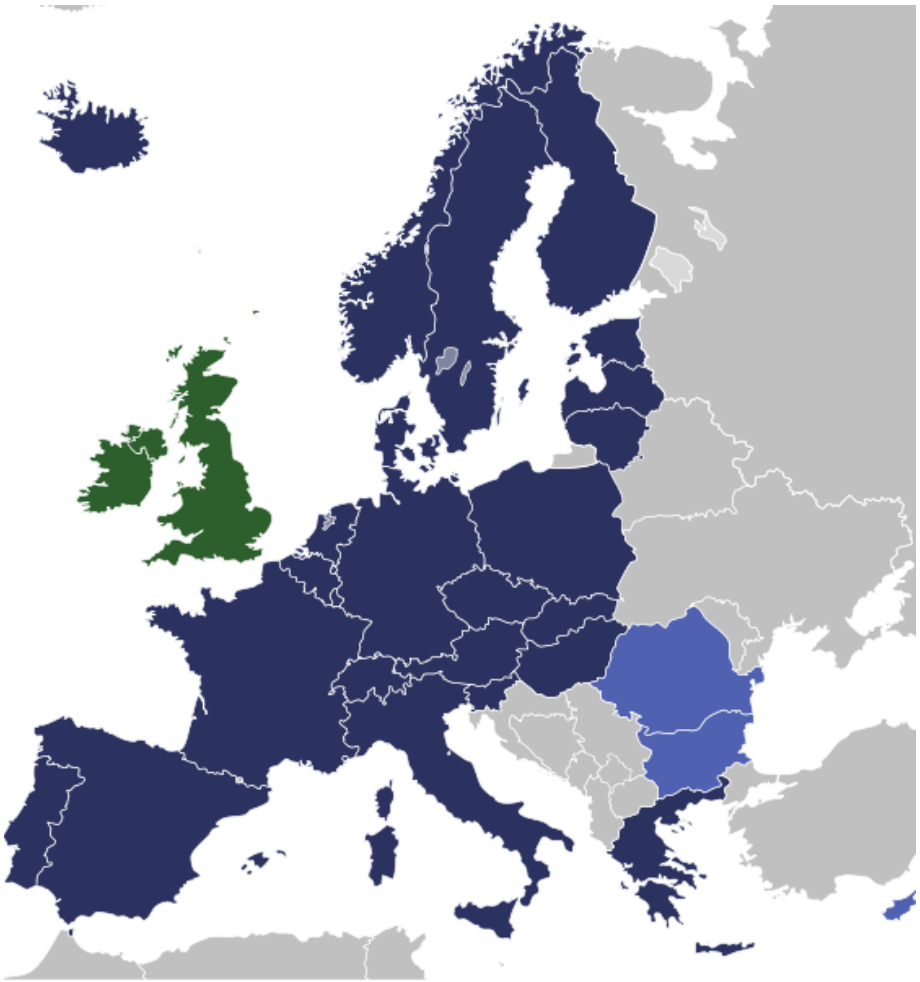
2. RAJATURVALLISUUS

Rajavartiolaki määrää Rajavartiolaitokselle tehtäväksi: ”Rajavartiolaitoksen toiminnan tavoitteena on rajaturvallisuuden ylläpitäminen” (Rajavartiolaki 1. luku 3 §) [32]. Arto Niemenkari määrittelee rajaturvallisuuden kirjassaan seuraavanlaisesti; ”Rajaturvallisuudella tarkoitetaan niitä rajavartiolaitoksen toimenpiteitä, joilla ennaltaehkäistään ja torjutaan erityisesti laitonta maahantuloa sekä osallistutaan valtakunnan sisäistä turvallisuutta vaarantavan rajat ylittävän rikollisuuden torjuntaan joko itsenäisesti tai yhteistyössä muiden kansallisten taikka muiden maiden viranomaisten kanssa[31].” Rajaturvallisuutta ylläpidetään tekemällä rajatarkastuksia rajavartiolain antamien toimivaltuuksien mukaisesti. Kun henkilö pyrkii Schengen-alueelle, hänelle tehdään rajatarkastus. Rajatarkastuksessa selvitetään henkilön henkilöllisyys sekä maahantuloedellytykset. Maahantuloedellytyksiä on muun muassa aito matkustusasiakirja, sekä ettei henkilöllä ole maahantulokieltoa.

Schengen-alue koostuu 26 Eurooppalaisesta maasta. Alueeseen kuuluu lähes kaikki Euroopan Unionin jäsenvaltiot. Iso-Britannia ja Irlanti ovat päättäneet olla liittymättä alueeseen ja Kypros on lykännyt liittymistään vuodella. Romanian ja Bulgarian, jotka liittyivät EU:hun vuonna 2007, on vielä jatkettava työtä turvallisuuskriteerien täyttämiseksi[7]. Schengen-sopimuksen piiriin kuuluvat myös Euroopan Unioniin kuulumattomat Norja ja Islanti, sekä Sveitsi ja Liechtenstein. Liechtenstein tosin ei vielä sovella Schengen-sopimusta ja Sveitsi liittyi maaliikenteen osalta soveltamaan

Schengen-sopimusta 12.12.2008, lentoliikenteen osalta sopimuksen soveltaminen alkaa keväällä 2009. Lisäksi Schengenin alueen sisällä ovat rajamuodollisuuksia ylläpitämättömät valtiot Monaco, San Marino ja Vatikaani, vaikka eivät olekaan allekirjoittaneet sopimusta. Näillä mailla on kahdenkeskiset sopimukset rajanaapuriensa kanssa, jotka ovat Schengenin sopimusmaita.

Nämä Schengen-sopimusta soveltavat maat eivät pidä sisärajatarkastuksia ollenkaan vaan keskittävät rajavalvonnan Schengen alueen ulkorajoille. Näiden maiden alueilla voi siis matkustaa maasta toiseen ilman passia ja rajatarkastuksia. Kun pääsee yhteen Schengen-maahan, pääsee kaikkiin Schengen-maihin. Tämän takia Schengen-alueelle on luotu yhtenäinen 4-portainen rajaturvallisuusmalli.



Kuva 1: Schengen-alue. Schengen-alue on merkitty tummansinisellä värillä. Vaaleansiniset maat eivät vielä sovella Schengen-sopimusta, vaikkakin ovat sen allekirjoittaneet. Vihreät maat soveltavat Schengen-sopimusta vain joiltakin osin [11].

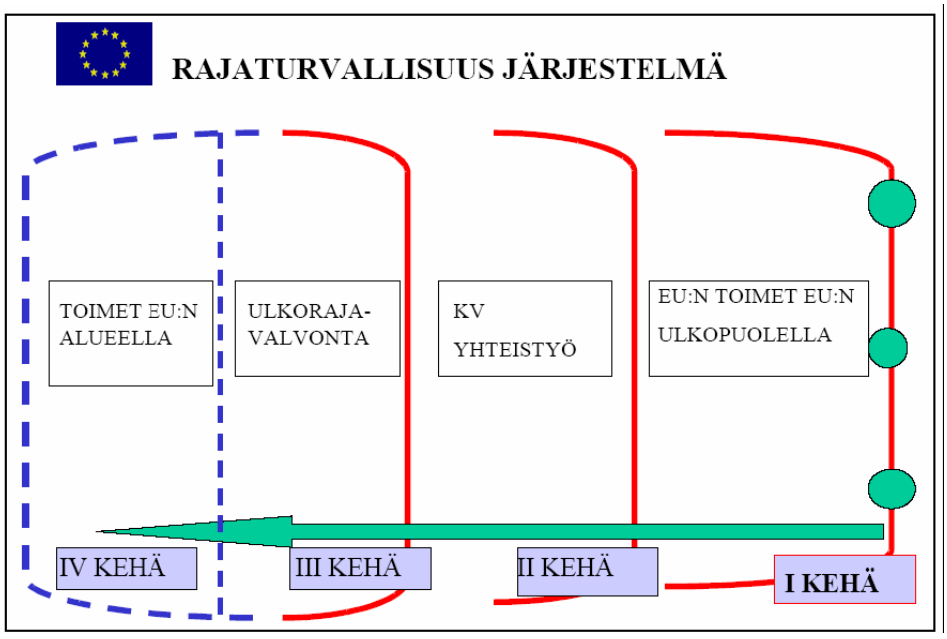
2.1 4 -PORTAINEN RAJATURVALLISUUSMALLI

Turvallisuuden säilyttämiseksi ja erityisesti laittoman maahantulon estämiseksi on luotu 4 -portainen rajaturvallisuusmalli. Malli on tehty koko Euroopan Unionille yhteiseksi Schengen-alueella toteutettavaksi rajaturvallisuusjärjestelmäksi, jolloin kaikilla jäsenmailla olisi näin ollen yhtenäinen malli. Yhtenäinen malli on erittäin tärkeää turvallisuuden kannalta, koska näin pystytään estämään mahdolliset rikollisten ja väärin perustein maahan pyrkivien kokeilut etsiä reitti Schengen-alueelle sellaisen maan kautta, jolla rajavartiointi on kevyemmin järjestetty tai viisumin myöntämisperusteet ovat löyhemmät.

Malli kuvaa eri toimintatasoilla toimeenpantavia toimia. Mallissa on huomattavissa rajatarkastusten painopisteen siirtyminen kylmän sodan aikaisesta rajalinjan turvaamisesta kauaksi itse varsinaiselta maantieteelliseltä rajalta lähtö- ja kauttakulkumaihin, joista on odotettavissa mahdollisia laittomia maahantulijoita.

4 -portaisen rajaturvallisuusmallin portaat ovat:

- EU:n toimet EU:n ulkopuolella
- kansainvälinen yhteistyö
- ulkorajavalvonta
- toimet EU:n alueella



Kuva 2: 4-portainen rajaturvallisuusmalli [31]

4-portainen rajaturvallisuusmalli on jaettu neljään kehään (ks. kuva 2). I-kehään kuuluvalla EU:n toimet EU:n ulkopuolella tarkoitetaan sitä, että rajatarkastukset aloitetaan lähtömaissa sijaitsevissa lähetystöissä. Sinne sijoitetaan asiantuntevaa henkilöstöä, jotka kykenevät havaitsemaan mahdollisia asiakirjaväärennöksiä, sekä tekemään henkilöllisyyden selvityksiä henkilön hakiessa viisumia. Tämä on tärkeää, jotta jo viisumia myönnettäessä saadaan estettyä väärillä tai väärennetyillä asiakirjoilla laittomasti Schengen-alueelle yrittävät henkilöt.

Myös liikkeenharjoittajille on annettu vastuuta. Schengenin yleissopimuksen 26 artiklan 1 kohdan b alakohta määrää liikkeenharjoittavat varmistumaan siitä, että maitse, tai meri- tai ilmateitse kuljetettavilla kolmannen maan kansalaisilla on vaadittavat matkustusasiakirjat mukanaan. Mikäli Schengen-alueelle pääsee henkilöitä, joilla ei ole vaadittavia matkustusasiakirjoja, ovat heidät Schengen-alueelle tuoneet liikkeenharjoittajat velvollisia palauttamaan kyseiset henkilöt lähtömaahansa.

Kansainvälisellä yhteistyöllä (Kuva2: II Kehä) tarkoitetaan käytännössä rajanaapureiden tekemiä keskinäisiä sopimuksia rajavalvonnan yhteistyöstä. Yhteistyö voi tarkoittaa esimerkiksi tietojen vaihtoa, rajavartijoiden yhteisiä partioita tai sopimalla erilaisia menetelmiä hätätilanteita varten, kuten esimerkiksi pelastusajoneuvojen liikkuminen rajan yli hätätapauksissa. Yhteistyösopimuksissa voidaan sopia myös virka-avusta asiakirjojen tutkimiseen. Esimerkiksi Venäjällä ei ole käytössä yhtä hyviä välineitä asiakirjojen tutkimiseen kuin Suomella, joten venäläiset rajavirkailijat voivat lähettää Suomen puolelle väärennökseksi epäilemiään asiakirjoja tutkittaviksi. Yhteistyöksi myös lasketaan eri tilanteiden hoitaminen neutraalilla tavalla poliittisten kiistojen välttämiseksi. Suomi ja Venäjä ovat sopineet maiden välille Rajajärjestyssopimuksen, jossa luodaan pelisäännöt pienempien rajarikkomusten hoitamiselle neutraalisti. Yhteistyön suunnittelussa on huomioitava myös mahdolliset merialueet ja niillä toimiminen.

III Kehän (Kuva2) mukaisella ulkorajavalvonnalla tarkoitetaan konkreettista rajavalvontaa valtion rajoilla. Schengen alueella ei sisärajatarkastuksia tehdä, niin tässä ulkorajalla tarkoitetaan Schengenin ulkorajaa. Keskeisimmät osa-alueet ovat seuraavat: 1) kaikki ulkorajan ylittävät henkilöt tarkastetaan systemaattisesti, ja 2) varmistetaan rajanylityspaikkojen välisen alueen tehokas valvonta. Näihin on puitteet määritelty Schengenin yleissopimuksen 6 artiklassa, joita sitten toteutetaan Yhteisen käsikirjan mukaisesti. Rajatarkastuksissa käytettävän laitteiston on oltava asianmu-

kaista, sekä henkilöstön oltava ammattitaitoista ja tarvittavin osin erikoiskoulutettua. Rajatarkastuksiin on oltava käytettävissä riittävät henkilöstöresurssit ja ammattitaitoinen henkilöstö. Jatkokoulutuksessa tulee huomioida muun muassa kielitaidon ja muuttuvan lainsäädännön tuntemuksen parantaminen.

Kaikkia kolmea rajatyyppiä (maa, meri ja ilma) koskevat erityisvaatimukset on tiedostettava ja täytettävä. Esimerkiksi lentoasemille on rakennettava erilliset linjastot Schengen- ja muille kansalaisille, etteivät he pääsisi sekoittumaan keskenään.

Toimilla EU:n alueella (Kuva2: IV Kehä) tarkoitetaan Schengenin sisällä tapahtuvaa maiden yhteistyötä kansainvälisen rikollisuuden torjumiseksi. Rikollisuus sekä maahanmuutto eivät kuitenkaan noudata maantieteellisiä rajoja. EU-mailla on oltava tämän takia keskinäinen tiedonjako selvillä. On mahdollista, että esimerkiksi jokin etsintäkuulutettu tekee rikoksen jossakin toisessa EU-maassa, jolloin rikollisen kiinniottavan maan viranomaisilla on oltava tieto rikollisen muista etsintäkuulutuksista. Joku turvapaikan hakija on voinut ilmoittautua ensin johonkin toiseen EU-maahan, mutta karannut sieltä toiseen EU-maahan, jossa taas esiintyy turvapaikanhakijana. Myös kielteisen turvapaikkapäätöksen saatuaan on mahdollista, että turvapaikanhakija siirtyy naapurivaltioon anomaan turvapaikkaa, kuten voisi esimerkiksi tapahtua Ruotsin käännyttäessä turvapaikanhakijoita. Tämänlaisten tapauksien takia on perustettu Schengen Information System (SIS). Sinne eri EU-maa kokoavat tietoa turvapaikanhakijoista ja etsintäkuulutuksista. EU:n ja Schengenin laajentuessa SIS on alkanut käydä liian pienimuotoiseksi ja ahtaaksi järjestelmäksi. Parhaillaan EU:ssa onkin kehittelyssä SIS II – järjestelmä, missä uudet maat ovat jo kehittelyssä mukana, jottei heidän tarvitsisi sitten muuntaa omia systeemejään vastaamaan SIS II – järjestelmää.

Schengen-valtio voi myös palauttaa sisärajatarkastukset määräajalle kansallisen turvallisuuden ja tilanteen niin vaatiessa, kuitenkin kuultuaan ensin muita Schengen-valtioita. Esimerkiksi Suomi palautti sisärajatarkastukset Euroopan turvallisuus- ja yhteistyöjärjestön ulkoministerikokouksen turvajärjestelyjen varmistamiseksi 24.11.–5.12.2008 väliseksi ajaksi. Sisärajatarkastusten palauttaminen aika-ajoin on ihan hyvä asia, sillä Schengen-alueen vapaa liikkuvuus koskee myös rikollisia ja laittomia maahanmuuttajia. Tästäkin Suomen järjestämästä vajaan kahden viikon kestäneestä sisärajatarkastuksista jäi tulokseksi yli 30 käännyttämistä ja 100 lievään valtioraja-

rikokseen syyllistynyttä henkilöä. Lisäksi Rajavartiolaitos aloitti kahden tapauksen yhteydessä laittoman maahantulon järjestämisen rikostutkinnan [13].

2.2 RAJATARKASTUKSET

Rajavartiolaki antaa yksiselitteiset puitteet missä ja milloin rajatarkastus toteutetaan. ”Rajatarkastus toimitetaan, kun henkilö aikoo ylittää ulkorajan tai hän on ylittänyt sen ilman rajatarkastusta. Rajatarkastus toimitetaan rajanylityspaikalla.”(Rajavartiolaki 578/2005 14 §) [32].

Rajavartiolaki määrittää myös rajatarkastukseen sisältyvät toimenpiteet tarkasti. Siinä säädetään, että ”Rajatarkastus toimitetaan joko vähimmäistarkastuksena tai, jos rajatarkastusta toimittavan viranomaisen tiedossa olevat seikat taikka vähimmäistarkastuksessa ilmenneet seikat antavat siihen aihetta, perusteellisena tarkastuksena. Vähimmäistarkastukseen sisältyy:

1. henkilöllisyyden selvittäminen rajan ylittämisoikeuden selvittämiseksi sekä maahantulokiellon, käännyttämispäätöksen tai maasta karkottamispäätöksen noudattamisen valvomiseksi ja etsintäkuulutuksissa pyydettyjen toimenpiteiden suorittamiseksi;
2. matkustusasiakirjan ja muun matkustusoikeutta osoittavan asiakirjan tarkastamisen rajanylittämisoikeuden selvittämiseksi sekä asiakirjan aitouden varmistamiseksi;
3. tarvittaessa henkilön kuuleminen;
4. tarvittaessa ajoneuvon kuljettajan ajokuntoisuuden ja ajoneuvon liikennekelpoisuuden valvonta.

Perusteelliseen tarkastukseen sisältyy vähimmäistarkastus. Lisäksi siihen voi sisältyä henkilöntarkastus sekä henkilön matkatavaroita ja kulkuneuvoa koskeva etsintä henkilöllisyyttä osoittavan tarpeellisen asiakirjan löytämiseksi ja sen varmistamiseksi, ettei henkilöllä ole hallussaan, matkatavaroissaan tai kulkuneuvossaan omaisuutta, joka on hankittu rikoksella tai tullut sellaisen omaisuuden tilalle, taikka muuta omaisuutta, jonka hallussapitoon tai rajan yli kuljettamiseen hänellä ei ole oikeutta.” (Rajavartiolaki 578/2005 19 §) [32]

Perusteellisten rajatarkastusten tekeminen on tehokasta, mutta hidasta sekä sursseja vaativaa. Mikäli rajanylittäjiä on paljon, jonot alkavat pian pidentyä ja odotusajat kasvaa. Liian pitkät jonotus- ja odotusajat voivat puolestaan aiheuttaa talouselämälle monenlaista haittaa. Turistit voivat kyllästyä jonottamaan pitkiä aikoja, ja siirtävät sitä välttääkseen matkojaan tulevaisuuteen tai kokonaan toiseen maahan. Rekat, jotka kuljettavat teollisuudelle tarvikkeita seisovat jonossa, vaikka niiden kuljettamien tarvikkeiden pitäisi saapua määränpäähän ilman pidempiä tarpeettomia viiveitä. Tilanne on sama laivoilla satamiin saapuvilla rekka-autoilla ja tavarankuljetuskonteilla, jotka joutuvat odottamaan käsittelyvuoroaan aikaa vievien rajamuodollisuuksien vuoksi. Koska suuri osa tuonnista kuitenkin tapahtuu rekoilla, on taloudellisesti kannattamatonta ylläpitää järjestelmää, joka aiheuttaa talouselämälle ylimääräisiä kustannuksia. Esimerkkinä tästä voi mainita Yhdysvaltojen rajavalvonnan tehostaminen syyskuun 11. päivän terrori-iskujen jälkeen. Rekkoja, kuten muutakin liikennettä alettiin tarkastaa niin perusteellisesti ja yksitellen, että vuoden 2001 syyskuun tuonti Kanadasta ja Meksikosta vajosi kolme miljardia dollaria alemmaksi kuin edellisenä vuonna. Yhdysvaltojen ja Meksikon välisen rajan läheisyydessä olevat vähittäismyyjät Yhdysvaltojen puolella ilmoittivat myynnin laskeneen 50 prosenttia vähentyneen meksikolaisen asiakaskunnan vuoksi [3].

2.3 UHKAKUVAT

Yhä kehittyvässä maailmassa ja terrorismin lisääntyessä rajaturvallisuuden ylläpitäminen on entistä haastavampaa. Ihmiset matkustavat entistä enemmän maasta toiseen, niin työ- kuin huvimatkoja. Rikollisilla on entistä paremmat resurssit maahantulon järjestämiseksi. Esimerkiksi syyskuun 11. päivän terrori-iskujen tekijät saattoivat tulla Yhdysvaltoihin yksinkertaisesti väärennetyllä opiskelija- tai turistiviisumilla. Rajavalvonnan painopisteen ollessa tuolloin lähinnä huumeiden ja laittomien siirtolaisten maahantulon ehkäisemisessä, terroristit saattoivat vain kävellä rajanylityspaikan läpi kenenkään siihen puuttumatta. Rajatarkastusten painopiste onkin tämän vuoksi siirrettävä vasta rajalla tapahtuvasta tarkastuksesta mahdollisten ongelmallisten matkustajien etukäteisseulontaan. Etukäteisseulonnalla pyritään paljastamaan ongelmalliset matkustajat jo lähtömaassa heidän hakiessa viisumia, ennen kuin he saapuvat kohdemaan rajatarkastukseen.

Miten sitten parantaa rajaturvallisuutta ilman, että normaalin liikenteen sujuvuus siitä kärsisi? Mielestäni olisi kehitettävä täysin uusi ja moderni menetelmä hyödyntäen nykyistä teknologiaa, joka vastaisi tämän päivän haasteisiin. Yksi vastaus tähän haasteeseen on automatisoidut rajatarkastukset, joita ollaan nyt kehittämässä myös Suomeen. Automatiikkaa hyödyntämällä rajatarkastuksissa on tavoitteena pyrkiä helpottamaan ruuhkia rajanylityspaikoilla sekä parantamaan yleistä turvallisuutta. Automatisoitujen rajatarkastusten kehittämistyössä voitaneen hyödyntää samantapaista rajatarkastusmenetelmää, jota Yhdysvalloissa käytetään, eli Smart Border. Smart Border soveltuu parhaiten kansainvälisille lentokentille ja satamiin, mutta osia siitä voidaan soveltaa myös maarajojen ylityspaikoille.

3. SMART BORDER

Smart Border -ajatusta on lähdetty kehittelemään syyskuun 11. päivän terrori-iskujen jälkeen. Yhdysvaltojen ja Kanadan välille haluttiin kehittää uudenlainen raja, joka vastaa 2000-luvun haasteisiin. Raja, joka mahdollistaa turvallisen ja vapaan rajan ylittämisen sekä ihmisille, että tavaroille. Raja, jonka yli on maailman suurin kahden maan välinen kauppakumppanuus. Raja, joka on luotettava terroristitoimintaa vastaan. Smart Borderin neljä tavoitetta onkin: varmistaa ihmisten rajanylitys, varmistaa tavaroiden ylikulku, varmistaa infrastruktuuri ja eri viranomaisten tiedonjako ja koordinointi [2].

Smart Border tarkoittaa uudenlaista tapaa tehdä rajatarkastuksia. Se on nimensä mukaisesti *älykäs rajatarkastustapa*. Valvonnan painopiste kohdennetaan matkustajien etukäteisseulontaan ja ongelmallisten matkustajien tunnistamiseen. Tärkeänä elementtinä automatisoituihin rajatarkastuksiin on tämän päivän huippuunsa kehittynyt teknologia ja sen tarjoamat mahdollisuudet. Matkustajat pystytään seulomaan jo ennen heidän saapumistaan rajanylityspaikoille. Uusien, entistä parempien, biometristen passien käyttöönotto, sekä parantunut informaatioteknologia lisäävät rajaturvallisuutta. Biometristen passien väärentäminen on perinteisiä passeja huomattavasti vaikeampaa, ellei jopa mahdotonta. Henkilöllisyyden todentamisesta tulee luotettavampaa, koska passeihin voidaan laittaa mikrosiruja, jotka sisältävät yksityiskohtaista tietoa passin omistajasta. Näin väärällä passilla maahan yrittävä henkilö jää välittömästi kiinni. Ennakkoseulonnassa paljastuneet ongelma- tai epäselvät tapaukset pystytään tunnistamaan nopeasti ja varmasti rajanylityspaikoilla biometristen

passien ansiosta. Biometrisistä passeista kerrotaan perusteellisemmin kappaleessa 3.2.

Smart Border on kehitetty riskianalyysin pohjalta. Riskianalyysissä analysoidaan maan rajoille ja sitä myöten koko maahan kohdistuvia uhkia terrorismista ja kansainvälisestä rikollisuudesta. Riskit ja terroriteot muutetaan matemaattisiksi laskutoimituksiksi helpottamaan niiden vertailua keskenään. Yksinkertaistettuna tehdään laskutoimituksia. Annetaan terroriteolle jokin arvo ennalta sovittujen periaatteiden mukaan ja kerrotaan se todennäköisyydellä:

Terroriteon riski (todennäköisyys)	x	Toteutuneen terroriteon seuraukset	=	Uhkan suuruus

Laskennallisesti suurimman arvon saanut uhka on luonnollisesti raskain yhteiskunnan kannalta. Uhkien vertailulla keskenään nähdään, mikä uhka vaatii minkälaisia toimenpiteitä ja varautumisia.

Laskutoimitusten analysointi ei kuitenkaan ole ihan yksikertaista. Mikäli jonkin terroriteon seuraukset olisivat todella tuhoisat, esimerkiksi terroristien räjäyttämä likainen ydinpommi, mutta sen toteutumisen todennäköisyys on todella alhainen, ei se välttämättä saa suurta todennäköisyyslukemaa. Toisaalta, mikäli taas jokin vähäisempi terroriteko on äärimmäisen todennäköinen, saa se puolestaan suuremman todennäköisyysarvon. Tämän vuoksi tarvitaankin todellisia, koulutettuja erikoisasiantuntijoita tekemään analyysia mahdollisista uhkista sekä rohkeita päätösvaltaisia henkilöitä, jotka päättävät mihin uhkaan vastataan milläkin tavalla.

Yhteiskunnan rakenne on viime vuosikymmenien aikana muuttunut huomattavasti. Kehittyneen informaatioteknologian monimutkaisuus ja modernisaatio tekevät riskien arvioinnista vaikeampaa kuin aikaisemmin. Yksittäisen terroriteon todennäköisyys voi olla pieni, mutta toteutuneen terroriteon seuraukset voivat olla valtavat. Hyvänä esimerkkinä jälleen kerran tuo syyskuun 11. päivän terrori-isku. Riskejä analysoidessa ja vertaillessa joudutaan jatkuvasti miettimään, kumpi on lopulta tärkeämpää: terroritekojen estäminen, vai hidastuneesta rajankulusta aiheutuneet mah-

dolliset taloudelliset sekä yhteiskunnalliset haitat. Yhteiskunnallisesti ajatellen sujuva rajan ylitys on tietenkin tärkeää. Rajoja ei kuitenkaan voida pitää täysin avoimina, joten on löydettävä sopiva kompromissi siihen.

Terrorismin uhkaa tiettyä maata tai kohdetta vasten on äärimmäisen hankala arvioida. Tavallinen rikostorjunta on huomattavasti helpompitajuista suurelle yleisölle. Rikollisuuden torjuntatyön onnistumista on helppo mitata vaikka näkyvien pidätyksien ja takavarikkojen määrällä. Kansalaiset kuitenkin odottavat terrorismin torjunnalta sadan prosentin onnistumisluokkaa. Mutta miten mitataan terrorismin torjunnan onnistumista? Terrorismintorjunnan ”onnistumiset” kun ovat harvinaisempia ja vaikeampi havainnoida. Kuinka esimerkiksi toteutumatta jääneitä terroritekoja voidaan mitata? Yksi ajatus tähän on esimerkiksi maassa vallitseva rauhan aika ja yleinen turvallisuuden tunne, jonka on aikaansaanut onnistunut rajavalvonta; mahdolliset rikolliset ja terroristit on pystytty pysäyttämään jo rajatarkastusten yhteydessä ja siten estämään toteuttamasta terrori-iskujaan. Tämä on Rajavartioviranomaisten tekemää näkymätöntä työtä.

Terrorismin torjunnassa on haasteena vaikea työ, suuret odotukset ja vaikeammat mittausvälineet. Jotta työ ainakin helpottuisi hieman, on Smart Border haluttu menetelmä ottaa käyttöön, Näin saadaan edes ne vähäiset terroriteot jäämään toteutumatta ja rikollinen aineisto pidettyä rajojen ulkopuolella.

Terroristiuhka yleismaailmallisella tasolla on noussut koko ajan ja rajojen pitäminen turvallisena vaikeutuu entisestään. Lähi-idän ongelmapesäkkeet ja siellä toimivat sota- ja rauhanturvaoperaatiot eivät todennäköisesti ainakaan laske terrorismin uhkaa operaatioihin osallistuvia maita kohtaan. Eikä Yhdysvallat ole enää terroristien ainoa kohde. Terroristijärjestö Al-Qaidaan kytköksissä oleva Irakin islamilainen valtioryhmittymä lupasi 100 000 dollarin palkkion ruotsalaisen taiteilijan Lars Vilksin päästä ja 50 000 dollaria Nerikes Allehanda -lehden päätoimittajan tappamisesta. Lehti julkaisi Vilksin piirtämän pilapiirroksen profeetta Muhammedista [23]. Myös Iso-Britannia ja erityisesti Lontoo on ollut terroristien kohteena useasti [22].

Kuten jo aikaisemmin todettiin, tehostettu rajavalvonta on hidas ja lisää ruuhkia rajanylityspaikoille. Rajoilla ei kuitenkaan saisi olla tarpeettomia esteitä lailliselle kaupankäynnille ja matkustamiselle. Niistä aiheutuu vaan ylimääräistä haittaa yhteiskunnalle ja taloudelle. Toisaalta ei rajoja täysin avonaisinakaan voida pitää. Olisi

aika noloa, jos terroristit ja rikolliset pääsisivät maahan helposti vain kävelemällä rajan ylitse.

Näin ei kuitenkaan ole, eikä tule olemaankaan. Smart Borderin kolme peruspilaria, seulonta, biometriikka ja informaatioteknologia ovat ne välineet, joilla Smart Borderin neljään tavoitteeseen päästään. Neljä tavoitetta ovat siis: ihmisten rajaylityksen varmistaminen, tavaroiden ylikulun varmistaminen, infrastruktuurin varmistaminen ja eri viranomaisten tiedonjako ja koordinointi. Tämä kaikki toteutuu Smart Borderilla rajaturvallisuudesta silti tinkimättä.

3.1 SEULONTA

Seulonnalla tarkoitetaan maahantulijoiden ennalta käsin tapahtuvaa tarkastamista. Kun henkilö hakee viisumia lähtömaassaan, hänen henkilöllisyytensä ja maahantuloedellytykset tarkastetaan, kuten aiemmin todettiin 4 -portaisen rajaturvallisuusmallin yhteydessä. Henkilöllisyyden tarkastamiseen kuuluu myös henkilön henkilöllisyyttä osoittavien asiakirjojen aitouden todentaminen. Ulkomailla sijaitseviin lähetystöihin tarvitsee siis sijoittaa teknistä tukea sekä väärennösten paljastamiseen kykenevää asiantuntevaa henkilöstöä ja panostaa näiden asiantuntijoiden koulutukseen. Asiantuntijoilla on myös hyvät mahdollisuudet tutkia paikallisia oloja ja siten lisätä tietämystään kyseisen alueelta tyypillisiin viisumin hakijoihin. Jo tällä tasolla pitäisi viranomaisilla olla pääsy erilaisiin rekistereihin. Esimerkiksi sormenjälkirekisteristä paljastuu, mikäli joku yrittää saada uutta viisumia eri henkilöllisyydellä, kuin millä on aiemmin esiintynyt. Mahdolliset epämääräiset tai vaaralliseksi luokitellut tapaukset pyritään näin ollen selvittämään jo lähtö- tai kauttakulkumaassa.

Seulonta ei lopu viisumin hakemisessa tapahtuvaan henkilöllisyyden selvittämiseen. Colin J. Bennett kuvailee teoksessaan *”What happens when you book an airline ticket?”* kuinka eri viranomaiset suorittavat lukuisia ennakkotarkastuksia henkilöistä ennen varsinaista maahan tulemista, varsinkin Yhdysvalloissa [33]. Vaikkakin Bennettin teos käsittelee enemmän tietoturvallisuutta, kertoo se silti tapauskohtaisen esimerkin ihmisestä, mitä kaikkea tietoja ja missä vaiheessa häneltä itseltään ja muista lähteistä kerättiin hänen matkustaessaan Torontosta New Yorkiin ja takaisin.

Matkustajista kerätään paljon tietoja eri rekistereihin matkan eri vaiheissa. Näitä rekistereitä rajavalvonta- ja muut turvallisuusviranomaiset tutkivat sillä aikaa, kun lentokoneella saapuvat matkustajat ovat vielä ilmassa. Esimerkiksi Yhdysvallat ja Kanada ovat Smart Borderiin liittyen sopineet jakavansa Advance Passenger Information (API) ja Passenger Name Records (PNR) rekistereiden tiedot lennoilla Yhdysvaltojen ja Kanadan välillä tarkoituksena identifioida kumpaan tahansa maahan tulevat riskiksi luokitellut matkustajat. Vuonna 2004 US Department of Homeland Securityn (DHS) johtaja Tom Ridge allekirjoitti sopimuksen, joka antaa Yhdysvaltojen rajaviranomaisten (Customs and Border Protectionin (CBP)) oikeuden kerätä PNR:n sisältämät tiedot kaikista lennoista EU:n ja Yhdysvaltojen välillä [7]. Tietoliikenneavaruuteen jää jokaisesta matkustajasta eräänlainen data-varjo tai digitaalinen persoona, jota viranomaiset sitten tarvittaessa jäljittävät. Kun tietoliikenneavaruudesta jäljitetään henkilöä, puhutaan myös digitaalisen sormenjäljen seuraamisesta. Tätä menetelmää on havainnollistettu esimerkiksi elokuvateollisuudessa muun muassa toimintaelokuvassa Die Hard 4.0, missä viranomaiset etsivät digitaalista sormenjälkeä jäljittääkseen tietoverkkoihin iskeneen hakkerin.

Jotta syntyisi käsitys kuinka laaja verkosto tietojen keruulle on muodostunut, seuraavissa kappaleissa käsitellään tarkemmin mitä nämä rekisterit oikein ovat.

3.1.1 COMPUTER RESERVATIONS SYSTEM

Computer Reservations System (CRS) on tietokoneistettu menetelmä, jota käytetään tietojen varastoimiseen, tietojen hakuun sekä helpottamaan yhteistoimintaa matkustamiseen liittyen. CRS:t olivat alun perin lentoyhtiöiden luomia järjestelmiä, joita on sittemmin laajennettu myös matkayhtiöiden käytettäväksi matkanvarausjärjestelmäksi. Suuria CRS:iä, jotka käyvät kauppaa monien lentoyhtiöiden kanssa, kutsutaan Global Distribution Systems:iksi (GDS). Lentoyhtiöt keskittävät suurimman osan lentojensa varauksista tiettyyn GDS:ään. Monet näistä järjestelmistä ovat nykyisin myös loppuasiakkaiden käytettävissä internetin välityksellä hotellien ja vuokra-autojenkin varauksiin, sekä muihin palveluihin pelkän lentolipun tilaamisen lisäksi.

Maailmanlaajuisesti on olemassa neljä suurta GDS:ää. Ne ovat Amadeus, Sabre, Galileo ja Worldspan. Sabre on perustettu jo vuonna 1960, ja muut kolme järjestelmää 80- ja 90-luvuilla. Eurooppalaiset lentoyhtiöt havaitsivat 80-luvulla silloiset matkanvarausjärjestelmänsä riittämättömiksi voimakkaasti lisääntyneen asiakasmäärän

vuoksi. Tämä johti Air Francen ja Lufthansan kehittämään yhteistyössä uutta jestelmää, Amadeusta, joka otettiin käyttöön vuonna 1987. On toki olemassa muitakin pienempiä GDS:iä, mutta nämä neljä tunnetaan maailmalla nimellä ”The Big Four”, eli Neljä Suurta. Onkin harvinaista, että jokin matkatoimisto toimisi ilman, että olisi missään tekemisissä minkään näistä Neljän Suuren kanssa.

Tietenkään tietotekniikan taso ei ollut perustamisaikana sillä tasolla, joka tänä päivänä on käytettävissä. Tilaukset toimitettiin tuolloin magneettikorteilla ja tarvittiin suuri henkilöstömäärä tekemään tätä työmäärää. Toimintatavat olivat toimivia silloiseen tilanteeseen, mutta lisääntyvä matkustajamäärä pakotti GDS:t hyödyntämään kehittynyttä teknologiaa kehittääkseen itselleen soveltuvampia järjestelmiä. Nykyisin Sabre, Amadeus ja Worldspan toimiikin jo pelkästään internet-pohjaisesti.

Seuraavassa taulukossa havainnollistetaan, että mikäli aikoo käyttää jonkin lentoyhtiön tai matkatoimiston palveluja, niin tiedot jää rekistereihin.

Nimi	**Kehittäjät**	**Muita käyttäjiä:**
Amadeus	• Air France • Iberia • Lufthansa • SAS	Johtavia internetissä toimivia matkatoimistot: • Amadeus.net • ebookers • Expedia • lastminute.com • Opodo • Rumbo Yli 150 lentoyhtiön verkkoasiakkaat mm. • Air France • British Airways • **Finnair** • Lufthansa • SAS Scandinavian Airlines System • Spanair • United Airlines

Sabre	• American Airlines Sabre on yhdistynyt suuren aasialaisen CRS:n kanssa, jonka kehittäjiä ovat. • All Nippon Airways • Cathay Pacific Airways • China Airlines • Singapore Airlines	• American Airlines • Malaysia Airlines • Alaska Airlines • Philippine Airlines • Pakistan International Airlines • Royal Brunei Airlines
Galileo	• Aer Lingus • Air Canada • Alitalia • British Airways • KLM • Swissair • TAP • US Airways	• United Airlines • CheapTickets • Ixeo
Worldspan	• Delta • Northwest • Trans World Airlines	• Expedia • Orbitz • TravelHero • Travelcom Worldwide • Hotwire • Priceline

Taulukko 1. Neljä Suurta Global Distribution Systems:iä vuonna 2007 [8].

Computer Reservations System on hyvä esimerkki tietojen jäämisestä tietoverkkoihin. Kaikesta jää jäljitettävä tieto data-maailmaan. Nykyään on vaikea mennä lennolle kenenkään tietämättä. Computer Reservations Systemien ja Global Distribution Systemsien avulla tiedetään kuka milläkin lennolla on menossa minnekin. Nämä tiedot tulisi olla rajavartijoiden saatavilla, kun tehdään rajatarkastuksia koneiden vielä ollessa ilmassa. Näin saadaan rajaturvallisuutta ulotettua ulommaksi 4-portaisen rajaturvallisuusmallin neljänneltä kehältä. Pelkkä tieto henkilöllisyydestä on vasta se tieto, jonka pohjalta voidaan aloittaa varsinainen rajatarkastus. Rajatarkastuksen tekemiseksi tarvitaan tarkat, yksilöivät tiedot henkilöstä. Passenger Name Record kertoo henkilöstä tarpeeksi tietoa, jotta varma tunnistaminen saadaan tehtyä.

3.1.2. PASSENGER NAME RECORD

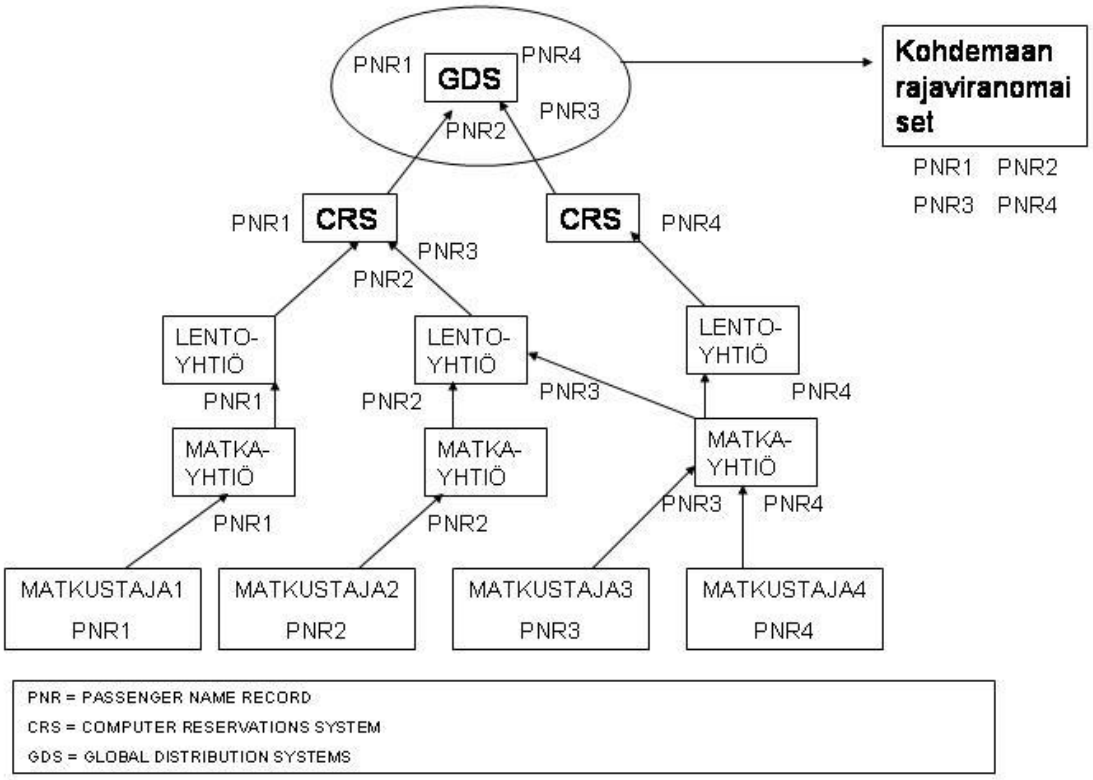
Passenger Name Record (PNR) on rekisteri, joka sijaitsee jonkin CRS:n tietokannassa. PNR sisältää matkustajan tai matkustajaryhmien matkatiedot. Lentoyhtiöt kehittivät PNR:n alun perin helpottamaan tiedon vaihtoa lentoyhtiöiden välillä, mikäli matkustajat tarvitsivat jatkoyhteyksiä eri lentoyhtiöiden lennoille päästäkseen lopulliseen määränpäähänsä. Tätä varten International Air Transport Association (IATA) loi standardit PNR:n sisällöstä ja ulkoasusta.

Kun matkustaja varaa itselleen lennon, luo matkatoimisto tai matkustajan käyttämä internet-sivu hänestä PNR-tiedoston siihen CRS:ään, mitä kyseinen matkatoimisto tai internet-palvelin käyttää. Tämä on tyypillisesti jokin näistä Neljästä Suuresta GDS:stä. Mikäli varaus on tehty suoraan lentoyhtiöön, PNR voi olla tallennettuna lentoyhtiön omaan CRS:ään. Tätä PNR:ää kutsutaan Master PNR:ksi. PNR identifioidaan tiettyyn tietokantaan Record Locatorilla.

Mikäli kyseinen Master PNR:n omistava lentoyhtiö ei voi itse tarjota kaikkia matkustajan tarvitsemia lentoyhteyksiä, lähettää lentoyhtiö kopiot PNR:stä lennon tarjoavan toisen lentoyhtiön CRS:ään. Nämä CRS:t tallentavat koko PNR tiedoston omiin tietokantoihinsa hoitaakseen heidän vastuullaan olevan matkan osan. Monien lentoyhtiöiden CRS on osa GDS:ää, joka mahdollistaa tietojen jakamisen.

Kopioitujen PNR tiedostojen Record Locatorit välitetään takaisin Master PNR:n omistavaan CRS:ään. Kaikki tiedostot siis linkittyvät yhteen. Tämä mahdollistaa tiedostojen päivittämisen, mikäli matka tai jokin muu tieto muuttuu jossakin CRS:ssä. Puhekielessä PNR:llä tarkoitetaan usein matkalipussa olevaa 6-merkkistä record locatoria, jolla PNR identifioidaan.

Seuraavassa kuvassa selvennetään, kuinka yksittäisen matkustajan passenger name record -tiedot liikkuvat järjestelmässä. Yksityiskohtaista tietoa matkustajista kulkee matka- ja lentoyhtiöiden, sekä computer reservation systemin kautta aina global distribution systemiin asti. Global distribution system on kuin suuri tietohautomo, jonka kautta saadaan kaikkien kohdemaahan lentokoneella matkustavien matkustajien tiedot. Siitä saadaan myös kaikkien tietyssä lentokoneessa tiettyyn kohteeseen matkalla olevien matkustajien PNR-tiedot kohdelentokentän rajavartiomiehille.



Kuva 3: Passenger name record -tietojen kulkeminen kohdemaan rajaviranomaisille

Teknisesti katsottuna PNR:ssä on viisi IATA:n määrittämää osaa, mitkä pitää olla täytettynä ennen varauksen lopullista onnistumista:

- matkustajan nimi
- matkatoimiston tai lentoyhtiön yhteystiedot
- matkalipun tiedot, numero tai voimassaoloaika
- matkareitti
- varauksen tehneen henkilön nimi

Nämä tiedot ovat vähimmäisvaatimus, mutta on paljon muitakin tietoja, joita matkatoimistot ja lentoyhtiöt vaativat varmistaakseen sujuvan matkustamisen. Näitä ovat:

- hintatiedot ja lipun mahdolliset rajoitukset
- maksutapa
- yhteystietoja, kuten koti- ja työpaikan osoite, puhelinnumero kotiin ja määränpäähän, sähköposti-osoite
- luottokortin tiedot

- ikä, mikäli sillä on merkitystä, kuten yksinmatkustavat lapset tai avustajaa tarvitsevat vanhukset
- ruoka- ja istuinpaikkatoivomukset, sekä muuta vastaavaa. Ruokatoivomuksissa voi esittää toiveita ruoasta, mikäli uskonto, terveydelliset syyt tai muut rajoitteet asettavat erityisvaatimuksia syömiselle.

PNR:ään voi lisätä myös lentobonuksia keräävien tiedot sekä mitä muuta tahansa tietoja, mitkä voi auttaa lentokentän henkilöstöä parantamaan asiakaspalveluaan.

Smart Borderiin liittyen monet valtiot ovat vaatineet lisää yksilöivien tietojen keruuta auttamaan tutkijoita jäljittämään rikollisia ja terroristeja. Näitä vaatimuksia ovat muun muassa

- matkustajan koko nimi pelkkien etukirjaimien sijaan
- passin tiedot (kansalaisuus, numero ja voimassaoloaika)
- syntymäpaikka ja -aika

PNR tiedostojen sisältämän laajan henkilökohtaisen tietomäärän onkin pelätty vaikuttavan ihmisten yksityisyydensuojaan. Tiedot matkustamisesta eivät nimittäin poistu tietokannoista ja ne voivat helposti muodostaa uudelleen tunnistettaviksi CRS:ien, matkatoimistojen ja lentoyhtiöiden toimesta, mikäli viranomaiset tarvitsevat jäljittää jonkun henkilön lentoreittiä, kanssamatkustajia, matkan rahoittajaa ja niin edelleen. Monilla CRS-GDS yhtiöillä onkin internet-sivustot, jotka mahdollistavat loppuasiakkailleen pääsyn omiin PNR tietoihin vain matkalipussa olevan varausnumeron perusteella.

Edellä mainitut uskonnon paljastavat ruokailutoiveet tai terveydentilan tiedot ovatkin Euroopan Unionissa ja joissain muissa maissa suojattua, arkaluontoista henkilökohtaista tietoa. PNR tiedot voivat paljastaa mistä henkilö on kotoisin, minne hän menee kuinka pitkäksi aikaa ja kenen kustannuksella. Vaikka tiedot sisältävät arkaluontoisiakin tietoja, niillä ei ole ainakaan vielä samankaltaista tietosuojaa, kuten pankkiyhteyksillä ja sairaskertomuksilla. Päinvastoin, niitä käytetään kuten tavallisia suoramarkkinointi tietoja.

3.1.3 ADVANCED PASSENGER INFORMATION SYSTEM

Advanced Passenger Information System (APIS) on perustettu lähinnä kaupallisia lentoyhtiöitä varten. APIS parantaa osaltaan rajaturvallisuutta, koska se antaa kohdemaan viranomaisille tietoja sinne tulevista matkustajista ja lentokoneen henkilökunnasta ennen lentokoneen varsinaista maahan saapumista. APIS on elektroninen tiedonvaihtojärjestelmä kahden tietokonejärjestelmän välillä; lentoyhtiön ja kohdemaan tietokonejärjestelmien. APIS sisältää perustiedot itse lennosta sekä yksityiskohtaista tietoa matkustajien passien sisältämistä tiedoista. Esimerkiksi Air Canadan mukaan Yhdysvaltoihin matkalla olevien matkustajien täytyy lähtöselvityksen yhteydessä täyttää API, joka sisältää seuraavat asiat:

- koko nimi
- sukupuoli
- syntymäaika
- kansalaisuus
- asuinmaa
- matkustusasiakirjan tyyppi, yleensä passi
- matkustusasiakirjan numero, voimassaoloaika ja myöntäjä
- osoite, jossa viettää ensimmäisen yön Yhdysvalloissa. (Ei vaadita yhdysvaltalaisilta tai asumisoikeuden omaavilta).

Varsinaisesti PNR- ja API-tietojen tarkastaminen ei vielä rajatarkastus. Niiden tarkastamisella päästään tunnistamaan henkilö varmasti. Rajatarkastuksen kannalta tosin on päästy vasta alkuun. Kun ensin on tarpeeksi tietoa ihmisestä, voidaan olla varma että kyseessä on juurikin yksi ja tietty henkilö, eikä esimerkiksi joku toinen samanniminen. Vasta tämän jälkeen voidaan tehdä varsinainen rajatarkastus eri rekistereitä hyväksi käyttäen. Rekistereistä kerrotaan lisää kappaleessa 3.3.

3.2 BIOMETRIIKKA

”Biometria on teknis-tieteellinen ala, jossa pyritään kehittämään yksilöiviä fysiologiaan perustuvia ihmisen tunnistusmenetelmiä. Biometrialla voidaan tarkoittaa myös yleisesti biologista mittaamista. Kreikan kielessä bios tarkoittaa elämää ja metron mittaamista” [10].

3.2.1 BIOMETRINEN TUNNISTAMINEN

Smart Borderissa biometriikalla tarkoitetaan lähinnä biometrisiä passeja ja henkilön biometrista tunnistamista. Sisäasiainministeriö määrittelee biometrisen tunnistamisen seuraavasti:

”Biometrinen tunnistus on ihmisen automatisoitua tunnistusta jonkin fyysisen ominaisuuden perusteella. Tutuin esimerkki biometriasta on sormenjälkitunnistus, jossa tietokone tunnistaa ihmisen hänen sormenjälkensä perusteella. Muita biometrisen tunnistuksen menetelmiä ovat esimerkiksi kasvontunnistus, äänentunnistus ja silmän iiriksen tunnistus.” [26] Silmän verkkokalvon tunnistus on myös yleinen biometrisen tunnistuksen menetelmä.

Automatisoiduissa rajatarkastuksissa pyritään siihen, että tunnistus voidaan toteuttaa kokonaan ilman ihmistä. Tunnistuksen suorittaa tietokone erilaisten laitteiden ja ohjelmistojen avulla. Automatisointi mahdollistaa suurten ihmismäärien tunnistamisen sujuvasti ja tehokkaasti.

Ennen biometriaan siirtymistä automatisoidun tunnistuksen menetelmiä ovat olleet esimerkiksi pankkikorteissa käytettävät tunnusluvut. Pelkkä tunnusluku ei kuitenkaan aina riitä riittävän luotettavaan tunnistukseen. Biometria parantaa ihmisen tunnistuksen luotettavuutta, sillä se kohdistuu suoraan ihmisen yksilöllisiin fyysisiin piirteisiin. Tunnusluvut ja salasanat voivat unohtua ja ovatpa ne myös alttiimpia varkauksille ja hakkeroinnille.

3.2.2 BIOMETRINEN PASSI

Biopassin kehittäminen sai alkunsa niin ikään syyskuun 11. päivän terrori-iskujen takia. Kuten aiemmin on todettu, se oli lähtölaukaus koko Smart Borderin kehittämistyölle, paremmalle rajaturvallisuudelle sekä sujuvammalle rajankululle. Smart Borderin konkreettisimpia toteutuksia on juuri biopassien käyttöönotto. Biopassit otettiin käyttöön elokuun lopulla vuonna 2006. Biopasseilla maahan tulevien ja maasta lähtevien ihmisten seuranta on helpompaa ja varmempaa. Ongelmana vain on se, että kuka määrittelee keitä ovat ne ”epäilyttävät” henkilöt, joiden liikkumista pitäisi valvoa. Valvonnan tulisi vielä tapahtua ilman, että rikotaan matkustajien oikeuksia ja yksityisyyden suojaa.

Biometrinen passi on ulkonäöltään samannäköinen kuin perinteinen passi. Ero perinteiseen passiin verrattuna biometrisessä passissa on henkilötietosivun sisään upotettu mikrosiru ja antenni. Mikrosirulle tallennetaan henkilötietoja kuten henkilön nimi, henkilötunnus, kansalaisuus, henkilön kasvokuva ja nimikirjoitus sekä digitaalinen allekirjoitus, joka sisältää mikrosirulle talletettujen tietojen tietoturvaan liittyviä tietoja. Biometrista passia pidetään äärimmäisen vaikeana, ellei jopa mahdottomana väärentää. Biometrisen tunnisteen sisältävän passin kannessa on tätä osoittava tunnuskuva.

Kuva 4: Biometrinen passi [14]

Kansainvälisen siviili-ilmailujärjestön (ICAO, International Civil Aviation Organization) on kehittänyt standardin biometriseen passiin. Sen mukaan kasvokuvan tulee sisältyä kaikkiin biometrisiin passeihin biometrisena tunnisteena. Standardi sallii myös iiriksen ja sormenjälkien käytön biometrisena tunnisteena. Biometrista passia koskeva asetus määrää Euroopan Unionin jäsenmaita ottamaan käyttöön biometrisina tunnisteina kasvokuvan ja sormenjäljen [9].

Passeissa käytettävä siru on kontaktiton RFID-siru (Radio Frequency Identification, eli radiotaajuinen etätunnistus), joten sitä ei tarvitse syöttää lukijalaitteen sisään. Pelkkä lukijalaitteen edessä käyttäminen riittää. Sirun muisti on vähintään 32 kilotavua ja siinä on useita prosessoreita. Siinä ei kuitenkaan ole omaa virtalähdettä, joten

se saa tarvitsemansa energia antenninsa kautta lukijalaitteesta. Sirua ja sirulla olevia tietoja suojataan lukuisilla turvaratkaisuilla [6].

Ennen kuin biometriset passit yleistyvät useissa maissa ainoaksi passimuodoksi on luultavaa, että näitä biometrisiä ominaisuuksia hyödynnetään normaalin passintarkastuksen tukena. Matkustajat tuskin huomaavat minkäänlaista eroa normaaliin passintarkastukseen verrattuna. Biometristen lukijalaitteiden yleistyessä biometristen passien rooli kuitenkin tulee kasvamaan vähitellen. Automaatiossa tuskin kuitenkaan päästään niin pitkälle, että voitaisiin perustaa kokonaan miehittämättömiä rajatarkastuspisteitä. Toimintahäiriöiden varalta tarvitaan vähintään perinteiseen rajatarkastukseen perustuva varajärjestelmä, eli ihminen tekemään manuaalisesti tarkastustyötä.

3.2.3 BIOMETRISEN PASSIN TIETOTURVA

Mutta ovatko biometriset passit niin turvallisia, kuin on annettu ymmärtää? Monet biometristen passien vastustajat kuitenkin kyseenalaistavat voimakkaasti ”huipputurvallisten” passien aukotonta tietoturvallisuutta. Tähän väitteeseen löytyy tukea seuraavasta esimerkistä:

Brittiläinen sanomalehti The Times pyysi kesällä 2008 Amsterdamin yliopiston tietoturvallisuustutkijaa Jeroen van Beekia murtamaan biometrisen passin [20]. Murtautumista varten van Beek tarvitsi vain kehittämänsä tietokoneohjelman, yleisesti saatavilla olevan sovelluskoodin palasen, 50 euron kortinlukijan sekä kaksi 13 euron hintaista rfid-sirua. Passin kloonaamiseen ja manipulointiin kului vain vajaa tunti. The Timesin mukaan van Beek kloonasi kaksi passeista poistettua sirua. Hän manipuloi niiden tietoja siten, että ne kelpasivat yhä kansainvälisen siviili-ilmailujärjestö ICAO:n lukijalle. Van beek vaihtoi pikkupojan passista tehdylle kloonisirulle terroristijohtaja Osama bin Ladenin kuvan, sekä 36-vuotiaan brittinaisen manipuloitu passin rfid-siru sai palestiinalaisen itsemurhapommittajan valokuvan. Van Beek kuitenkin toteaa, ettei hän väitä, että terroristit pystyisivät tekemään tämän kaikille passeille tai että he pystyisivät siihen huomenna. Tähän on kuitenkin syytä suhtautua tilanteen vaatimalla vakavuudella ja sen pitäisi herättää julkista ja avointa keskustelua passien turvallisuudesta ja asianomaisten tulisi ryhtyä toimenpiteisiin tiedostettujen väärinkäytösmahdollisuuksien estämiseksi ajoissa.

Van Beek on yliopistotutkija, joka onnistui murtamaan biometrisen passin. Myös hakkeriryhmä The Hacker's Choice väittää murtaneensa biometrisen passin helposti[19]. Verkkosivuilleen lataamassa videossa tämä hakkeriryhmä näyttää selkeästi, miten peukaloitu passi kelpaa hollantilaisella lentokentällä sijaitsevalle automaatille. Videolla näkyvän automaatin mukaan väärentämättömänä pidetty passi näyttäisi kuuluvan vuonna 1977 menehtyneelle Elvis Presleylle. Jotta muille hakkereille olisi passien murtaminen entistä helpompaa, hakkeriryhmä ikään kuin yllyttääkseen tai kiusallaan julkaisi ohjelmiston, jolla voi tehdä varmuuskopion passin mikrosirusta. Ryhmä on vahvasti sitä mieltä, että biometriset passit tuudittavat meidät valheelliseen turvallisuuden tunteeseen. Vaikkakin passi meni läpi tästä hollantilaisen lentokentän automaatista, niin tapauksesta uutisoinut Brittiläinen tietotekniikkalehti PC Pro kuitenkin muistuttaa, ettei kyseessä ole rajaviranomaisten käyttämä automaatti. Videon katsomisen perusteella jokainen voi myös todeta saman. Passi kyllä kelpaa automaatille, mutta siinä ei ole minkäänlaista avautuvaa porttirakennetta, joten se ei ole rajatarkastuksiin tarkoitettu portti.

Suomalaisia biometrisia passeja pidetään kaikesta huolimatta äärimmäisen luotettavina. Sisäasiainministeriön biometriahankkeen projektipäällikkö Tero Tammisalon mukaan eri maiden biopasseissa on eroja. Hänen mukaansa suomalaispassien tietojen manipulointi ei ole käytännössä mahdollista[20]. ”Passin sirulla olevien tietojen vaihtaminen siten, että meidän passin yksilöintivaiheessa tekemämme sähköinen allekirjoitus täsmäisi yhä, ei ole mahdollista”, täsmentää Tammisalo. Tammisalon mukaan Suomen valitsemat algoritmit ja salausavainten pituudet ovat sellaisia, etteivät passien peukaloiminen ole mahdollista. Suomalaispassien käyttämän, julkiseen avaimeen perustuvan PKI-järjestelmän (PKI = Public Key Infrastructure, eli kasvokuvan ja perustietojen salaamiseen käytettävä salausjärjestelmä. Passeihin tulossa oleva sormenjälki salataan eri järjestelmällä) murtaminen vaatisi niin paljon laskentatehoa, että se on käytännössä mahdotonta, Tammisalo vakuuttaa.

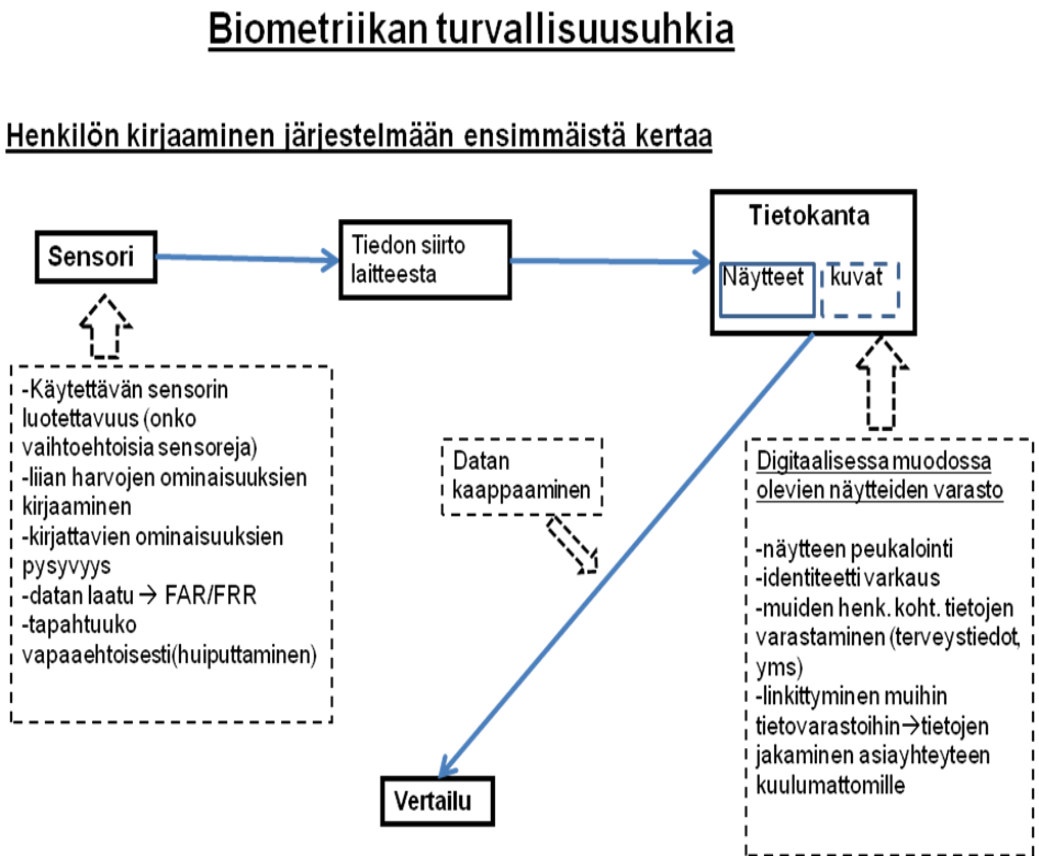
Suomalaiset biometriset passit ovat siis ainakin tämänhetkisen tiedon mukaan murtovarmoja. Muiden maiden passeista on toisaalta vaikea mennä takuuseen. Mitä tämä sitten hyödyttää? Mitä hyötyä on Suomella olla murtovarma biometrinen passi, jos muilla mailla ei ole? Biometristen passien ideahan nimenomaan on juuri siinä, että ne sisältävät yksilökohtaista tietoa passin kantajasta ja ettei tietoja voi väärentää. Tällöin voidaan olla varmoja, että passien kantajat ovat juuri niitä keitä väittävätkin olevansa, ja rajatarkastuksia voidaan nopeuttaa automaateilla. Tällainen tieto vie

kieltämättä pohjaa biometristen passien uskottavuudelta. Täytyy kuitenkin muistaa, että van Beek on yliopiston tietoturvallisuustutkija, jolla on käytettävissään erinomaiset resurssit, kuin myös se, että The Hacker's Choicen huijaama automaatti ei ollut rajaviranomaisten käyttämä automaatti. Matkustajamäärän kasvaessa ei vaihtoehtoja juurikaan ole ja joitain toimenpiteitä on yksinkertaisesti automatisoitava, jotta henkilöstöä saataisiin muihin tehtäviin. Biometrinen passi kuitenkin on tällä hetkellä ylivoimaisesti paras ja luotettavin mahdollinen vaihtoehto kaikkine tällä hetkellä tiedossa olevine vikoineen, kun puhutaan automatisoiduita rajatarkastuksista.

3.2.4 BIOMETRIIKAN TURVALLISUUSUHKIA

Biometrinen järjestelmä on muutakin, kuin matkustajan, biometrisen passin ja automaattisen rajatarkastusportin muodostama kolminaisuus. Biometrisiä järjestelmiä on olemassa vaikka kuinka erilaisia. Jotta systeemi toimisi muunakin kuin automaattisena oven avaajana, on paljon erilaisia asioita mitä tulee tehdä. Mikäli kuitenkin puhutaan pelkästään rajatarkastuksiin liittyvistä biometrisista systeemeistä, niin niiden ei tarvitse olla niin kaiken moniosaisia, kuin joidenkin muihin tarkoituksiin käytettävien biometristen järjestelmien. Biometrista tunnistustahan voidaan käyttää esimerkiksi virastotaloissa sisään pääsemiseksi pelkästään sormenjäljellä avaimen sijasta, tai kuten Filippiinien sosiaalitoimisto käyttää biometrisia tunnisteita asiakkaiden tunnistamiseksi ja väärillä henkilöllisyyksillä haettavien korvauksien huijausyritysten karsimiseksi[16]

Biometrisessä järjestelmässä on kuitenkin omat haavoittuvuutensa. Tuskinpa mikään järjestelmä maailmassa on täysin aukoton. Ei myöskään biometrinen järjestelmä. Tällä hetkellä olemassa olevista järjestelmistä biometrinen järjestelmä kuitenkin lienee turvallisin vaihtoehto. Seuraavissa kuvissa on esitetty mitä kaikkia turvallisuusuhkia tai toimintavarmuutta haittaavia tekijöitä biometriseen järjestelmään voi liittyä.



Kuva 5: Biometriikan turvallisuusuhkia henkilön järjestelmään kirjautumiseen liittyen.

Jotta biometrisesta tunnisteesta olisi jotain hyötyä, tulee siihen olla vertailukohde. Vertailukohde tulee siitä, kun henkilö ”luodaan” ensimmäistä kertaa järjestelmään. Esimerkiksi biometrisessa passissa henkilöstä otettu kasvokuva muutetaan digitaaliseen muotoon. Suomalaisiin biometrisiin passeihin on vuonna 2009 tulossa myös sormenjälki kasvokuvan lisäksi.

Kasvokuvan ottamisessa päästään ensimmäiseen toimintavarmuutta aiheuttavaan tekijään. Ainakin nykyisin on passia hakevan henkilön mahdollista ottaa itse passiin tuleva kuva ja toimittaa se passin myöntävälle viranomaiselle (Suomessa poliisille). Passikuvalle on laadittu tarkat määräykset, millainen kuvan tulee olla. Mutta olisiko silti syytä harkita vaihtoehtoa, että olisi vain tietty viranomainen, joka ottaisi kaikki kuvat samalla menetelmällä ja samanlaisilla laitteilla. Näin pystyttäisiin takaamaan kuvien tekninen samankaltaisuus ja varmistamaan, että kaikille passinhakijoille tulisi samoilla standardeilla otettu kuva. Myös kuvien uusintaotokset tai niiden teknisen tason säätäminen viranomaisten toimesta vähenisi. Kuvan laatu on erityisen tärkeä tunnistamisen kannalta. Huonolaatuiset tai vaikka vähän huonosta asennosta otetut

kuvat aiheuttavat vain turhia hylkäyksiä tai vääriä hyväksymisiä. Näitä kutsutaan nimillä False Acceptance Rate (FAR) eli väärien hyväksymisien aste, sekä False Rejection Rate (FFR) eli väärien hylkäämisten aste. Jo se, että tapahtuuko kuvan ottaminen vapaaehtoisesti, vaikuttaa lopputulokseen. Mikäli henkilö on pakotettu antamaan itsestään yksilöllisiä tunnisteita, voi hän helposti esimerkiksi kurtistamalla kulmia tai huonolaatuisella kameralla kuvan ottamalla vaikuttaa kuvan laatuun.

Lisäksi henkilön luomisessa on olennainen asia otetaanko oikeita biometrisiä tunnisteita huomioon. Biometriset tunnisteet ovat toki yksilöllisiä ja suhteellisen pysyviä. Mutta mikäli otetaan pelkkä kasvokuva, niin kuinka paljon voi esimerkiksi plastiikkakirurgialla vaikuttaa henkilön tunnistettavuuteen. Esimerkiksi Iltalehti uutisoi 18.12.2008 Yhdysvalloissa tapahtuneesta kasvojensiirtoleikkauksesta, jossa onnettomuuden uhriksi joutuneen naisen kasvoista korvattiin 80 % siirteillä[25]. Oikeiden tunnisteiden ottamisen lisäksi olisi suotavaa ottaa enemmän kuin yksi tunniste. Jälleen kerran tunnistettavuus paranee, kun on useampia tunnisteita yhden tunnisteen sijaan, mikä voi antaa vääriä hylkäyksiä tai hyväksymisiä. Useamman tunnisteen tapauksessa useamman tunnisteen täytyy vastata, joten väärien hylkäyksien ja hyväksymisien riski laskee.

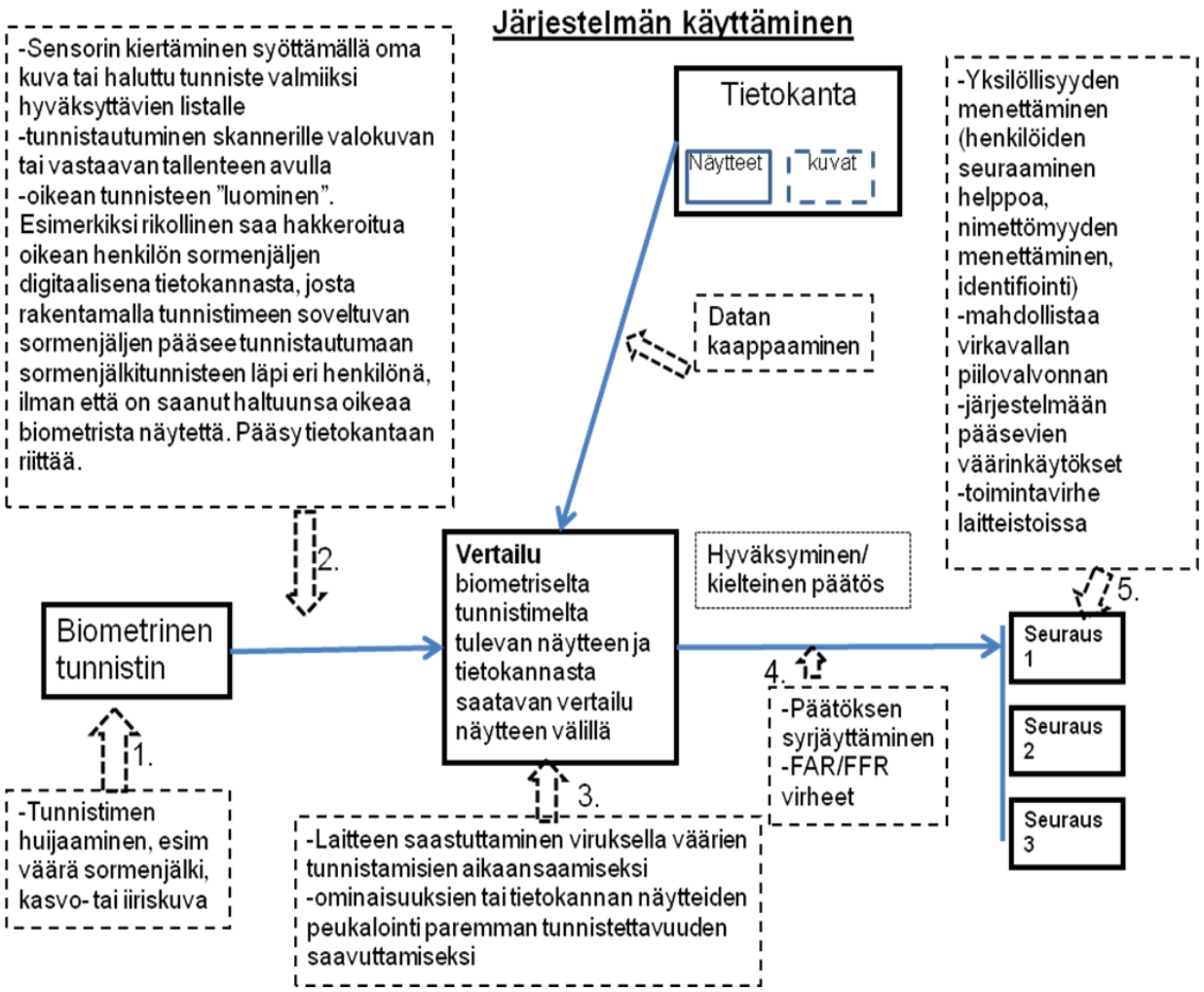
Tietojen säilyttämiseen käytettävä tietokanta on jo itsessään lievä uhka turvallisuudelle; tiedothan on joka tapauksessa säilytettävä jossain. Biometristen passien kanssa varsinaista tietokantaa ei ole, vaan tieto on passin sisällä olevassa sirussa. Mutta, onko se pelkästään siellä, vai onko jossain muualla jonkinlaisia piilotietokantoja viranomaisten valvonnan helpottamiseksi? Tietokanta pyritään tietenkin suojaamaan mahdollisimman hyvin kaikenlaisilta hyökkäyksiltä. Kun yhdessä paikassa on paljon tietoa lukuisista eri ihmisistä, ja nykyaikanahan tieto on valtaa, niin tämä valtaisa määrä erilaista tietoa sisältävä tietokanta saattaa houkutella rikollisia kuten pankkiholvien rahapinot aikoinaan houkutteli rosvoja villissä lännessä.

Tietomurtoon päässeen rikollisen mahdollisuudet identiteettivarkauksiin tai muihin omaa rikollista toimintaa edistävään toimintaan riippuvat tietokannasta (tietokannan sisältämästä tiedosta) ja rikollisen henkilökohtaisista kyvyistä. Elokuvateollisuus ideoi usein tulevaisuuden mahdollisuuksia ja fantasioita ja niinpä erilaisissa elokuvissakin on ollut esillä monenlaisia identiteettivarkauksia. Esimerkkeinä näistä vaikka Sandra Bullockin The Net – Verkko Kiristyy vuodelta 1995 identiteettivarkauden

osalta tai televisiosarja Alias, missä muokataan jonkun oikean, tietokannan mukaisen henkilön kuva omaksi kuvaksi, jotta biometrinen tunnistin päästäisi läpi. Tiedon ja teknologian kiihtyvässä vauhdissa voi vain arvella todellisen elämän tietokonehakkereiden mahdollisuuksia vastaavanlaisiin tekoihin.

Biometrisiä järjestelmiä kehittelevät ja valmistavat yhtiöt vakuuttavat omien laitteidensa olevan täysin murtovarmoja. Mutta kuten aikaisemmin on jo todettu tämän tieteenalan olevan erittäin nopeasti kehittyvä ja muuttuva, järjestelmien valmistajien on pystyttävä takaamaan, että nämä laitteet ovat tulevaisuudessakin yhtä murtovarmoja, kuin laitteen myyntihetkellä. Vaikka valmistajiin voisikin luottaa, valitettavaa kuitenkin on, että joidenkin viranomaisten luotettavuus voi joskus olla kyseenalainen. Aika ajoin julkisissa tiedotusvälineissä on kerrottu joidenkin viranhaltijoiden kiinnijäämisistä erilaisista vakoilu- tai lahjontatapauksista tai muista väärinkäytöksistä. Tietokantoihin ei tietenkään pidä olla ’kaikilla kaikkeen’ vapaa pääsyoikeus ja viranomaisillakin vain virkatehtävään liittyvään aineistoon. Mutta kun on käsillä valtava määrä tietoa, voi kiusaus vaikkapa katsoa oman naapurin tietoja käydä liian suureksi.

Järjestelmään käyttämiseen liittyy luonnollisesti enemmän turvallisuusuhkia, kuin ensimmäiseen turvallisuusuhkaan eli kirjautumiseen tai henkilön luomiseen. Seuraavassa kuviossa on esitetty järjestelmän käyttämiseen liittyviä turvallisuusuhkia.



Kuva 6: Biometriikan turvallisuusuhkia järjestelmän käyttämiseen liittyen

Biometrista tunnistinta voidaan pahimmillaan huijata jopa niinkin yksinkertaisesti, kuin esittämällä väärä sormenjälki tai kasvokuva (1. kohta).

Todennäköisin riski kuitenkin lienee kuvion kohdassa 2. esitetty väärinkäytöksen ennakoitu ilmenemismuoto. Mikäli biometrinen skanneri ei ole tarpeeksi hyvä eli validoitu toimimaan sille tarkoitetulla tavalla, niin tällöin skanneri voi hyväksyä pelkästään sille esitetyn kuvan kasvoista tai silmän iiriksestä tai mitä nyt kulloinenkin laite sattuu kysymään. Toinen tähän kategoriaan liittyvä uhkakuvan mahdollisuus, ja jota myös itse pidän todennäköisimpänä vaihtoehtona oikeassa elämässä, on näytetty havainnollisesti lukuisissa elokuvissa: hakkeri murtautuu tietokantaan ja peukaloi valmiita näytteitä itselleen sopivaksi tai vaihtoehtoisesti luo itsensä järjestelmään. Tämä on todellinen ja vakavasti otettava uhka, sillä rikollisen ei välttämättä tarvitse edes saada käsiinsä oikean henkilön biometrista tunnistetta, pelkästään pääsy tietokantaan riittää. Pahimmassa tapauksessa riittää tietokantanäytteen digitaalinen mal-

li, josta saa tehtyä itselleen tekosormenjäljen tai vaihdettua oman sormenjäljen lalle. Tämän kaltainen tietomurto on esitetty lukuisissa elokuvissa, mutta on toki pidettävä mielessä, että elokuvat ovat elokuvia ja mielikuvituksen tuotetta, eivätkä välttämättä kuvasta lähimainkaan todellisuutta tulevaisuudessa saati sitten nykyhetkestä. Yhteiskunta kehittyy ja teknistyy ja tiede menee eteenpäin kuitenkin huimaa vauhtia. Monet keksinnöt alkavat pienistä harmittomista ja uteliaista kokeiluista ja kohta huomataan, että se, mitä eilen pidettiin mahdollisena vain valkokankaalla, on tänään arkipäivää todellisuudessa.

Kohdassa 3. kuvataan sellaista toimintaympäristöä, jossa lähes kaikkea liikennettä, ei pelkästään tietoliikennettä, hallinnoidaan tietokoneilla. Tietokonevirukset ovat nykyisin arkipäivää. Tietokoneita ei kuitenkaan välttämättä tarvitse uhata virus, että järjestelmät kaatuvat aiheuttaen suurta haittaa. Huhtikuussa 2008 Sampo Pankissa tehtiin laaja tietojärjestelmien vaihto suomalaisesta järjestelmästä emoyhtiön Danske Bankin kanssa yhteiseen järjestelmään. Tämä valtava ohjelmien ja tietokantojen siirto- ja yhdistelyprojekti ei kuitenkaan sujunut ongelmitta ja epäonnisten vaiheiden seurauksena verkkopankki meni nurin kymmeniltä tuhansilta asiakkailta muutaman päivän ajaksi ja ohjelmien toimivuuksia korjailtiin vielä useita kuukausia sen jälkeenkin. Tietokonevirukset aiheuttavat kuitenkin enemmän ongelmia, koska tietojärjestelmien vaihtoja ei tehdä tuon tuosta. Mikäli biometrisen systeemin vertailua tekevä osa saastuisi viruksilla, olisi se äärimmäisen tuhoisaa koko systeemin toimimisen ja sen olemassaolon kannalta. Lisäongelmia tähän tuo vielä se, ettei virus edes välttämättä näy heti, vaan tekee ensin laajempaa tuhoa piilossa. Lisäksi vertailua tekevälle laitteelle voi aiheuttaa ongelmia muokkaamalla näytteistä hankalasti tunnistettavia tai niistä voi tehdä todella samankaltaisia.

Kohdassa 4. on FAR/FFR virheet. Nämä laitteistolle ominaiset pienet virheet, kuten tunnistusherkkyys, voivat käydä suurten massojen hallinnassa loppujen lopuksi aika suuriksi. Esimerkiksi Australiassa olevassa SmartGate kasvojentunnistinportissa tulee vääriä hylkäyksiä 2 % tapauksista ja 0.1 % pääsee läpi virheellisesti [15]. Prosentit tuntuvat pieniltä, mutta kun muutetaan prosentit matkustajamääriksi, nämä pienet prosentit konkretisoituvat suuriksi ihmismääriksi. Australian lentokentillä kulkee vuosittain noin 20 miljoonaa matkustajaa (Australian Customs and Border Protection Servicen, Australian tulli- ja rajapalvelu) [18]. 2 prosenttia 20 miljoonasta matkustajasta on 400 000 väärin hylättyä matkustajaa ja 0,1 prosenttia 20 miljoonasta matkustajasta on 20 000 väärin perustein hyväksyttyä matkustajaa. Tietenkään

kaikilla näillä 20 miljoonalla matkustajalla ei ole kyseisessä SmartGate portissa vaadittavaa ePassia, joten kaikki eivät käytä porttia. Mikäli tulevaisuudessa olisi visio automatisoida rajatarkastukset lentokentillä ympäri maailman, ei tämän suuruusluokan virhemarginaaleihin mielestäni ole varaa. 99,99 % tunnistamistodennäköisyys tuntuu korkealta, mutta vaikka prosentuaalisesti todennäköisyys tunnistettavuudelle on lähes 100, miljoonien matkustajamäärien kyseessä ollessa, on virhemarginaali 0,01% vielä liian suuri, varsinkin kun näihin lukuihin sisältyy myös niitä väärin perustein liikkuvia matkustajia.

Laite, joka suorittaa vertailun tietokannan tietojen ja tunnistimelta tulevien tietojen välillä, tekee päätöksen; joko kyllä tai ei. Päätöksestä riippuu, mitä seuraavaksi tapahtuu: henkilö joko pääsee läpi tai ei. Tähänkin laitteen tekemään päätökseen hakkerit voivat pyrkiä vaikuttamaan siten, että laite tekee juuri päinvastaisen päätöksen mitä pitäisi, tai että saisivat mahdollisuuden laitteen tekemän päätöksen kumoamiseen. Päätöksen kumoamisella tarkoitetaan, että vaikka laite antaisikin kielteisen päätöksen, niin silti hakkeri pystyisi kumoamaan tai hylkäämään päätöksen ja avaamaan portin.

Kun automatisointi menee niin pitkälle, että kaikki toiminta tapahtuu tietokoneilla, on yksilön valvonta helpompaa. Automaattisten porttien käytöstä rekisteröityy sähköinen jälki, loki-merkintä ja viranomaiset pystyvät näkemään, kuka missäkin kulkee. Tälle parjatulle ”isoveli valvoo” käsitteelle löytyy kuitenkin suuri joukko vastustajia. Vastustajat perustelevat mielipiteensä sillä, että yksilöllisyys katoaa, eikä enää pystytä olemaan osa harmaata massaa. Tässä vaiheessa on muistettava, että terroristithan nimenomaan haluavat piiloutua harmaaseen massaan. Yksilön valvonta on siis kahdenjakoinen asia. Toisaalta valvonta luo turvallisuutta, toisaalta se vähentää yksityisyyttä.

3.3 INFORMAATIOTEKNOLOGIA

Informaatioteknologialla tarkoitetaan Smart Borderin yhteydessä viranomaisten yhteistyötä, automaattista tietojen vaihtoa ja eri rekistereiden käyttöä automatiikkaa hyödyntäen. Jotta viranomaiset voisivat toimia mahdollisimman tehokkaasti, heillä tulee olla resursseja matkustusasiakirjojen ja henkilöllisyyden selvittämisiin. Kuten

aikaisemmin tässä tutkielmassa on todettu, rajavalvonta alkaa jo lähtömaassa. Kun henkilö hakee viisumia kohdemaan lähetystöstä, hänen henkilöllisyytensä selvitetään. Mikäli viisumia myöntävällä viranomaisilla lähtömaassa ei ole pääsyä esimerkiksi Schengen Information System -tietojärjestelmään (SIS) tai SIS II – tietojärjestelmän kanssa kehitteillä olevaan Viisumitietojärjestelmään (VIS, Visa Information System), on vaikea selvittää, voiko tälle matkalle lähtijälle myöntää viisumia vai ei. Henkilöllähän voi olla maahantulokielto johonkin toiseen Schengen valtioon, kuin mihin hän hakee viisumia. Sisärajatarkastuksia kun ei Schengen-alueella ole, pääsisi henkilö näin siihen valtioon, mihin hänelle on määrätty maahantulokielto. Schengen Information System on vain yksi esimerkki kansainvälisistä tietokannoista, joihin useat Euroopan maat tallentavat tietoja henkilöistä liittyen rajaturvallisuuteen ja rikostorjuntaan.

Jokaisella maalla on kuitenkin myös omia kansallisia tietokantoja. Suomessakin on Poliisilla ja Rajavartiolaitoksella erilaisia tietokantoja, kuten poliisin tietokanta sormenjäljistä tai etsintäkuulutuksista sekä Rajavartiolaitoksen tietojärjestelmä. Kun sormenjälkitietojen lisääminen biometrisiin passeihin alkaa, tulee siitäkin oma tietokanta. Lisäksi on olemassa lukuisia muita tietojärjestelmiä, jotka liittyvät enemmän tai vähemmän rajatarkastuksiin, kuten esimerkiksi puhelinyhtiöiden tietokannat asiakkaistaan tai viestintäviraston tietokanta TV-luvan maksaneista henkilöistä. Kaikki tietokannat eivät tietenkään liity rajatarkastuksiin, mutta niitä voidaan tarvita esimerkiksi rikostutkinnassa. Poliisilla olisikin suurta kiinnostusta saada käyttöoikeus tulevaan sormenjälkirekisteriin, koska siinä olisi muidenkin ihmisten, kuin vain tunnettujen rikollisten sormenjäljet.

Jokaisella maalla tulisi periaatteessa olla kaikkien muiden maiden kansallisetkin rajaturvallisuuteen liittyvät tietojärjestelmät käytössään. Schengen Information Systemiin kun on mahdoton kirjata kaikkea tarvittavaa tietoa järjestelmän paisuessa muutenkin uusien jäsenmaiden myötä. Tämä onkin perimmäinen syy, miksi on alettu kehittämään Schengen Information system II:sta. Tietojenvaihdon paraneminen on askel kohti parempaa rajaturvallisuutta ja sitä myöten koko Schengen-alueen tutkimusta.

Sama tiedonvälityksellinen ongelma mikä on lähtömaassa, toistuu kohdemaassa. Kohdemaassa on kuitenkin eri viranomaiset, jotka tekevät rajatarkastuksen ja tullitarkastuksen, tai valvovat yleistä järjestystä ja turvallisuutta. Viranomaisilla tulee olla

pääsy kaikkiin tarvittaviin rekistereihin, mitkä voivat liittyä asiaan, ja uskallus käyttää niitä. Esimerkkinä tästä voi mainita tapauksen, jossa Vaalimaan rajatarkastusasemalla oli kiinalainen laiton rajanylittäjä vuonna 2007. Kyseinen henkilö oli tulossa taksilla Haminasta Vaalimaan rajanylityspaikalle, kunnes matkalla tuli taksikuskin kanssa erimielisyyksiä kyydin maksamisesta. Paikalle kutsuttiin poliisi, joka selvitti tilanteen ja taksi kyyditsi kiinalaisen rajanylityspaikalle. Sieltä tämä kiinalainen mies lähti kävelemään metsää pitkin kohti Venäjää. Valvontakamerat paljastivat rajan ylittämisen. mutta sen jälkeen ei hänen liikkeistään ole mitään jälkiä. Mikäli poliisi olisi tehnyt heti ilmoituksen rajanylityspaikalle epämääräisestä taksilla liikkujasta, olisivat rajanylityspaikan rajamiehet voineet olla valmiina vastaanottamassa tätä liikkujaa ja tekemään rajatarkastuksen. Näin ei kuitenkaan käynyt. Nyt kiinalainen katosi Venäjän puolelle, eikä hänestä tiedetä sen enempää, kuka hän oli ja mihin menossa. Edellä kuvatun esimerkin on kertonut Virolahden rajavartioalueen päällikkö majuri Pasi Marttisen esittelyluennollaan Virolahden rajavartioalueesta kadeteille 11.9.2007 Virolahden rajavartioalueen johtopaikalla [34]. Mieleenpainuva esimerkki siitä, kuinka eri viranomaisten olisi tehtävä enemmän yhteistyötä rajaturvallisuuden ylläpitämiseksi.

4. AUTOMATISOIDUT RAJATARKASTUKSET KÄYTÄNNÖSSÄ

Tämän hetkisen käsityksen mukaan automatisoidut rajatarkastukset soveltuvat parhaiten kansainvälisille lentokentille, kuten Suomen tapauksessa Helsinki-Vantaan Lentoasemalle. Automatisoitujen rajatarkastusten ydin on ennakkoseulonnassa ja jo lähtömaahan asti ulotettavissa tarkastuksissa. Lähtömaassa viisumia hakiessa henkilön taustat tarkastetaan maahantulokelpoisuuden selvittämiseksi. Lentokoneen noustessa ilmaan lähtömaassa, matkustajatiedot välittyvät kohdemaahan sähköisesti tietojärjestelmiä pitkin. Kohdemaassa tehdään henkilöistä hakuja eri viranomaisten rekistereihin ja tietojärjestelmiin, jotta voitaisiin seuloa tarkempaa tarkastelua vaativat matkustajat heidän ollessa vielä ilmassa. Tässä tarkastuskierroksessa viranomaisilla on oltava käytössään kaikki mahdolliset rekisterit ja tiedostot, jottei mitään olennaista jäisi huomaamatta, esimerkiksi mahdollisten rikosepäilyjen vuoksi olevia etsintäkuulutuksia jossain muussa Schengen-maassa. Lentokoneen laskeutuessa kohdemaahan ja matkustajien saapuessa rajatarkastukseen, on kaikkien taustat jo selvitetty hyödyntäen uudenlaisia ja luotettavia biometristen passien yksityiskohtaisia tunnistetietoja. Etukäteisselvityksessä ilmenneet tarkempaa tarkastusta vaativat ta-

paukset voidaan tunnistaa vaivatta ja nopeasti biometriikan ansiosta normaalin rajatarkastuksen yhteydessä ja nämä henkilöt voidaan ohjata sivuun tarkempaa tarkastusta varten. Automatisoidut rajatarkastukset parantavat rajaturvallisuutta, tarkastusten luotettavuutta ja nopeuttavat tavallisten matkustajien matkustamista – nämä kun voivat vain kävellä linjastoa pitkin ja vilauttaa biometristä passiaan lukijalaitteessa. Tarkastukset on tehty etukäteen, ja lukijalaite vain toteaa, että passia kantaa oikea passin haltija.

Maaraja-asemilla ei ole käytössä ennakkoilmoitus-menetelmää saapuvista matkustajista. Ainoa ennakkoseulonta, mikä on käytössä, on viisumia haettaessa ollut taustojen selvitys. Junaliikenteessä ja säännöllisillä rekkakuljetuksilla voidaan soveltaa automatisoituja rajatarkastuksia sellaisenaan, jos vain on mahdollista tehdä ennakkoilmoitus. Rekkajonoja Suomesta Venäjälle Kaakkois-Suomen rajanylityspaikoilla tämä tuskin lyhentää, sillä siellä olevat viivytykset eivät johdu Suomen Rajavartiolaitoksesta. (Tilastojen mukaan Suomi pystyy syöttämään rekkoja rajatarkastuksesta läpi nopeammin, kuin mitä Venäjä kykenee ottamaan niitä vastaan. Tämä julkaisematon tieto on peräisin Virolahden rajavartioalueen päällikkö majuri Pasi Marttisen esittelyluennolta Virolahden rajavartioalueesta kadeteille 11.9.2007 Virolahden rajavartioalueen johtopaikalla [34].)

Tavallinen autoileva matkustaja, joka saapuu autolla rajanylityspaikalle, ei yleensä anna saapumisestaan ennakkoilmoitusta. Automatisoidut rajatarkastukset eivät välttämättä nopeuta näitä tapauksia, sillä rekistereistä tapahtuva tarkastus voidaan suorittaa vasta henkilön saapuessa rajanylityspaikalle ja siinä paikan päällä odottaessa. Hyöty, joka näissäkin tapauksissa saadaan automatisoimalla rajatarkastusta, on kuitenkin se, että rajatarkastusta tekevällä viranomaisella on tuolloin käytettävissään rekisterit ja muut sähköiset tietokannat, jotka nopeuttavat tiedonhakua ja siten tarkastus nopeutuu. Biometrinen passi toimii tässäkin tapauksessa luotettavana tunnistusvälineenä, koska sen avulla saadaan varmuus siitä, että henkilö on juuri se, joka väittääkin olevansa.

Tällä hetkellä Euroopan Unionissa on päästy automatisoitujen rajatarkastusten osalta sille tasolle, että erilaisia automaattisia passintarkastusportteja on otettu koekäyttöön joissakin Euroopan maissa. Mitään yhtenäistä linjaa ei kuitenkaan vielä ole tullut Eurooppalaisille lentokentille tuleville porteille. Kaikissa porteissa on kuitenkin yksi yhteinen tekijä, portti on kaksiosainen. Ensin matkustajan tulee syöttää biomet-

rinen passi lukijalaitteeseen, mikä avaa ensimmäisen oven portista päästäen matkustajan portin kahden oven väliseen tilaan. Tässä tilassa tapahtuu automaattinen ja biometrinen tunnistaminen. Järjestelmistä riippuen tunnistaminen voi tapahtua kasvokuvan perusteella, jossa kamera vertaa matkustajan kasvokuvaa biometrisen passin sirulla olevaan digitaaliseen kasvokuvaan. Lisäkriteerinä voidaan käyttää niin sanottua kolmen kuvan vertailua. Kolmen kuvan vertailussa laite vertaa sirulla olevaa kuvaa skannattuun passin nimiösivulla olevan kuvaan ja vielä sirulla olevaa kuvaa kameran ottamaan kuvaan. Tunnistaminen voi tapahtua myös iiriksen tai sormenjäljen perusteella. Kun portti on tunnistanut matkustajan passin haltijaksi, eikä rekistereistä ole ilmennyt estettä maahanpääsylle, avautuu portin toinen ovi ja matkustaja pääsee tästä porttien välitilasta jatkamaan matkaansa. Seuraavissa kappaleissa tarkastellaan automatisoitujen rajatarkastusten tilannetta Suomen lisäksi joissakin muissa maissa, jotta saisimme käsityksen, missä tänä päivänä mennään.

4.1 AUTOMATISOIDUT RAJATARKASTUKSET SUOMESSA

Tutkimuksen kirjoittamisen aikana automatisoidut rajatarkastukset ovat Suomessa edenneet jo pelkästä suunnittelusta kokeiluasteelle. Helsinki-Vantaan lentoasemalle otettiin automaattiset passintarkastuslaitteet, passiautomaatit, koekäyttöön 8.7.2008 [14]. Kokeilun tarkoituksena on selvittää automaattisen rajatarkastuksen soveltuvuutta Schengenin ulkorajalla suoritettaviin rajatarkastuksiin. Käytännön tavoitteita ovat asiakirjaturvallisuuden entistä tehokkaampi hyödyntäminen sekä rajatarkastuksista vapautuvan henkilöstön kohdentaminen tarvittaviin keskeisiin tehtäviin.

Rajavartiolaitoksen kannalta on edullista tarjota mahdollisuutta matkustajille sujuvaan itsepalvelutarkastukseen. Tärkeää on myös kerätä kokemuksia automatisoinnista ja edelleen kehittää rajaliikenteen sujuvuutta jatkuvasti lisääntyvistä matkustajamääristä ja tasaisena pysyvistä määrärahoista huolimatta. Kokeilusta saatavien tulosten perusteella käyttöä valmistaudutaan laajentamaan Helsinki-Vantaan lentoaseman lisäksi itärajan kansainvälisille rajanylityspaikoille.

Rajavartiolaitos itse määrittelee Internet-sivuillaan olevassa tiedotteessa tisen rajatarkastuksen seuraavasti: *”Automaattinen rajatarkastus on matkustajan omatoimisuuteen perustuva menetelmä, jossa matkustajan henkilöllisyys ja asiakirjan aitous varmistetaan hyödyntämällä voimassaolevaa passia ja sen sirulta saatavia tietoja.”*

Matkustajan toimiminen passiautomaatilla on hyvin yksinkertaista. Tarkastuslinjalle saapuessaan (vaihe 1 kuvassa alla) matkustaja asettaa ensin voimassaolevan biometrisen passinsa lukijalaitteeseen, joka lukee asiakirjan tiedot. Seuraavaksi (vaihe 2) laite vertaa reaaliajassa kasvokuvaa sirulla olevaan kuvaan. Tarkastuslinjalla voi olla vain yksi matkustaja kerrallaan.

Kuva 5: Passiautomaatti Helsinki-Vantaan lentoasemalla [14]

Automaatin käyttöön liittyy luonnollisesti tiettyjä rajoitteita. Automaatissa ollessa ei ole sallittua peittää kasvojaan millään lailla tai käyttää päähineitä, aurinkolaseja tai mitään elektronisia laitteita, kuten esimerkiksi mp3-soittimia.

Automaattisen rajatarkastusjärjestelmän varmistettua matkustusasiakirjan aitous sekä biometrisen tunnistamisen jälkeen matkustaja voi jatkaa matkaansa. Mikäli matkustaja tai passi ei täytä tarvittavia ehtoja tai tunnistaminen on epäonnistunut, matkustaja siirtyy käyttämään perinteistä rajatarkastuslinjaa.

Tämän hetkinen Helsinki-Vantaalla kokeilukäytössä oleva linjasto ei välttämättä ole se lopullinen linjasto, mikä Suomeen aiotaan ottaa, mutta kuitenkin varteen otettava vaihtoehto. Vastaavanlaisia automaattisia rajatarkastuksia hyödynnetään muun muassa Portugalin Lissabonissa, Farossa ja Funchalissa ulkorajatarkastuksissa sekä erityisjärjestelyin Pariisin, Frankfurtin ja Amsterdamin lentoasemilla etukäteen rekisteröityneille matkustajille [21].

4.2 AUTOMATISOIDUT RAJATARKASTUKSET MAAILMALLA

Eri maat ovat alkaneet ottaa käyttöönsä erilaisia, toisista maista poikkeavia, automatisoituja rajatarkastusmenettelyjä. Kuten aikaisemmin todettiin, Euroopassa ei ole olemassa mitään yhtenäistä linjaa siitä, millaisia automaattien pitäisi olla. Itse asiassa Euroopan Unionin asetukset määräävät vain, että mailla tulee olla ICAO:n (ICAO, International Civil Aviation Organization) standardien mukainen biometrinen passi ja sen, mitä kaikkea rajatarkastukseen liittyen voidaan automatisoida. Koska määräykset eivät sisällä sääntöä miten automatisointi tulee järjestää, jotkin maat ovat kehitelleen omanlaisia sähköisiä tai elektronisia passeja sekä kulkukortteja, joiden tarkastaminen perustuu automatiikkaan. Yleisesti maailmalla puhutaan joko biometrisista passeista tai ePasseista, jotka käytännössä tarkoittaa samaa. On olemassa myös erilaisia SmartCard tyyppisiä henkilökortteja, jotka eivät kuitenkaan ole passeja.

Aikaisemmin kappaleessa 3.2.4 mainittuun Australian SmartGate portteihin tarkoitettu ePassport vastaa suomalaista biometrista passia. Australian SmartGate toimii tällä hetkellä kuitenkin vain Australian ja Uuden-Seelannin ePasseilla. Myöhemmin SmartGaten käyttöä laajennetaan koskemaan myös muita kansallisuuksia, kunhan heillä vain on ICAO:n standardien mukainen biometrinen tai elektroninen passi. SmartGate tekee tunnistuksen passissa olevan digitaalisen kasvokuvan perusteella samoin kuin Suomessa koekäytössä oleva Portugalista tullut passiautomaattikin. Australian automaatissa on vain kolme kameraa eri korkeuksilla, joiden kaikkien ottamista kuvista laite valitsee parhaiten tunnistukseen soveltuvan kuvan. Automaatti ei ole varsinaisesti yhteydessä mihinkään tietokantaan. Sekä Australiassa että Suomessa olevat portit siis perustuvat saman biometrisen ominaisuuden tunnistami-

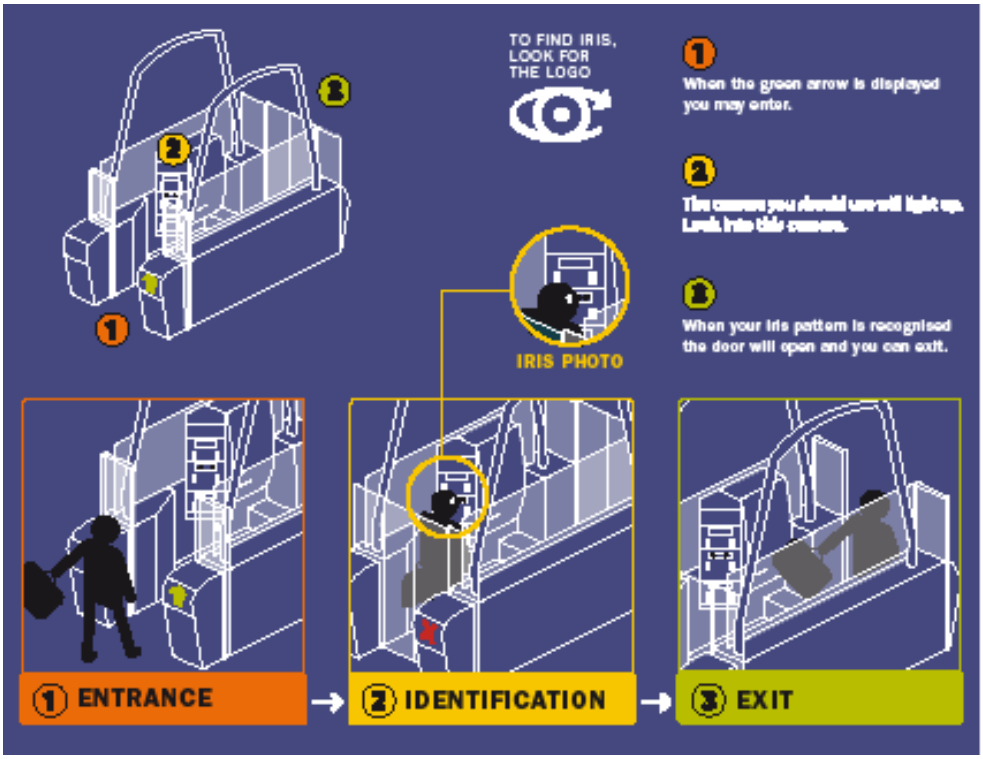
seen, mutta ovat vain eri valmistajan tekemiä. Tulevaisuus näyttää kumpi malli toimii paremmin, vai kenties molemmat yhtä hyviä.

Kuva 6: Australian SmartGate kasvontunnistusjärjestelmällä [17]

Ranskalaisilla viranomaisilla on koekäytössä P.E.G.A.S.E. niminen järjestelmä automatisoituihin rajatarkastuksiin liittyen. P.E.G.A.S.E. tulee sanoista Experimental Programme for Secure Automated Access Control; eli vapaasti suomennettuna kokeellinen ohjelma turvalliseen ja automaattiseen sisäänpääsyn kontrolloimiseen. PEGASE toimii erillisellä SmartCard –kortilla. Portti on tarkoitettu nopeuttamaan paljon matkustavien henkilöiden asiointia lentokentällä. Korttia on pitänyt hakea erikseen, eikä se ole sama asia kuin passi, vaan eräänlainen henkilökortti. Korttiin tulee nimi, osoite, syntymäaika ja sormenjälki. Portissa tunnistaminen tapahtuukin juuri sormenjäljen perusteella. Portti vertaa sormenjälkeä kortin sormenjälkeen. Näin pyritään varmistamaan, ettei yksikään etukäteen kirjautumaton asiaton henkilö pääse porttien läpi varmistetulle alueelle [24].

Kuva 7: PEGASE –järjestelmän SNG 770 portti sormenjäljen lukijalla [12].

Isossa-Britanniassa on käytössä IRIS -niminen järjestelmä. IRIS tulee sanoista Iris Recognition Immigration System, eli iiriksen tunnistamiseen perustuva järjestelmä. Iiris, samoin kuin sormenjälki on yksilöllinen, koska kenelläkään toisella ihmisellä ei ole toista samanlaista iiristä. IRIS järjestelmä, kuten edellä mainittu PEGASE, vaatii etukäteen rekisteröitymisen järjestelmään. UK Border Agencyn (Iso-Britannian rajavartioinnista vastaava viranomaistaho) mukaan järjestelmään pystyy reksiteröitymään täysi-ikäiset ihmiset lähes samoin perustein, kuin saisi viisumin Iso-Britanniaan. Myös Euroopan Unionin kansalaiset voivat rekisteröityä tähän järjestelmään. Järjestelmään rekisteröityessä kuvataan matkustajan iiris, joka vie noin viidestä kymmeneen minuuttia aikaa. Digitaalinen iiris-kuva sitten siirretään tietokantaan muiden rekisteröityneiden iiris-kuvien kanssa. Kun matkustaja sitten saapuu portille, ottaa laite hänen iiriksestään kuvan ja vertaa sitä koko tietokantaan. Etukäteen rekisteröitynyt matkustaja ollessaan tulossa Iso-Britanniaan voi UK Border Agencyn mukaan päästä IRIS-portin läpi vain noin 20 sekunnissa [29].



Kuva 8: IRIS -järjestelmän portti iiris-skannerilla [30].

5. VERTAILU

Automatisoidut rajatarkastukset ovat Suomessa, ja oikeastaan koko maailmassa, vielä niin alkuvaiheissa, että varsinaista vertailua automaattisten ja rajavartijan tekemien rajatarkastusten välillä on vaikea tehdä. Koekäytössä oleva passiautomaatti on testausvaiheessa, jossa testataan onko se ylipäänsä soveltuva Suomen olosuhteisiin. Maailmallakaan ei vielä ole valmista mallia olemassa. Porteissa on vielä ”lapsentauteja” ja niiden käyttö on muutenkin ollut suhteellisen vähäistä, joten niistä ei vielä ole saatu tarkoitettua hyötyä irti. Tällä hetkellä käytettävissä olevista tuloksista voi lähinnä vain päätellä, mitä pitäisi olla toisin, jotta järjestelmä saataisiin kunnolliseen operatiiviseen käyttöön ja automatisoinnille asetetut tavoitteet toteutettua [35]. Automatisoidut rajatarkastukset ovat ideana hyvä, mutta tällä hetkellä vielä savolaista humoristista ilmaisua käyttääkseni ”toteutusta vaille valmis” – vaiheessa.

Kuva 9: Passiautomaattien linjasto Helsinki-Vantaan lentoasemalla [14].

Automatisoinnilla pyritään siis vähentämään rajatarkastuksiin sitoutuvaa työvoimaa, jolloin voitaisiin siirtää työvoimaa rajatarkastuksista muihin painopistealueisiin rajatarkastuksista sekä parantamaan turvallisuutta. Tällä hetkellä matkustajien rajatarkastusten nopeutumisen ei voi sanoa toteutuneen. Teknisiä virheitä, sekä muita sujuvaa käyttöä haittaavia virheitä on niin paljon, etteivät portit juurikaan houkuttele ihmisiä. Koska kyseessä on lisäksi uusi laite, joka voi aiheuttaa hämmennystä, eivätkä matkustajat välttämättä tiedä, kuinka portissa tulisi toimia, voivat matkustajat aiheuttaa näitä virhetilanteita itsekin tahattomasti. Portti on mekaaninen laite, jossa kamera yrittää ottaa ihmisestä kuvaa. Mikäli ihminen ei seiso oikeassa kohdassa tai katselee väärään suuntaan, kestää myös kameralla tarpeettoman kauan aikaa hakea tunnistettava kuva. Mikäli käytetään kolmen kuvan vertailua ja passi on huonosti lukijassa, eikä skanneri saa kunnolla skannattua nimiösivun kuvaa, seurauksena voi olla tarkastuksen hidastuminen. Hitaaksi käynyt tarkastus puolestaan turhauttaa ennestään epätietoiset ihmiset ja se aiheuttaa vain kohtuutonta uuden systeemin väheksymistä. Tämä onkin tällä hetkellä ongelman ydin, sillä yhtenä tavoitteena on juuri ollut tavallisten matkustajien tarkastusten nopeuttaminen. Lisäksi, koska Euroopan Unionin kansalaisista ei tehdä rekisterihakuja kuin satunnaisesti, niin automaatissa voi yhden matkustajan huolimaton esiintyminen kameran edessä kestää tarpeettoman kauan aiheuttaen turhia jonoja. Toisaalta, kun Euroopan Unionin kansalainen tulee rajavartijan luukulle ja hänen ojentaessaan passinsa rajavartijalle, näkee kokenut rajavartija hyvinkin nopeasti muutamissa sekunneissa, että passi on voimassa ja edessä seisoo passin osoittama henkilö. On mahdollista, että luukullakin voi välillä kestää, mutta tällöin hidastumisen syy voi olla siinä. että rajavartijan

kokemuksen myötä tullut sisäinen intuitio pysäyttää hänet tarkastamaan jotkut mat-matkustajat tarkemmin kuin toiset.

Tavallisen matkustajan tarkastuksen nopeutumisen lisäksi tärkeimpänä automatisoinnin tavoitteena on ollut turvallisuuden parantaminen. Tätä tavoitetta on lähestytty biometrisilla passeilla, joista ainakin suomalaisten kehittämiä malleja pidetään mahdottomina väärentää. Biometrinen tunnistaminen on aina varmempi, kuin silmämääräinen, sillä biometriset ominaisuudet ovat yksilökohtaisia ja uniikkeja piirteitä eri ihmisillä.

Tällä hetkellä suomalaisissa biometrisissä passeissa oleva ja koekäytössä olevan passiautomaatin biometrinen tunnistaminen perustuu pelkkään kasvokuvaan. Onko kasvokuva siten yksinään kyllin riittävä peruste tunnistaa henkilö? Tämä seikka voidaan perustellusti kyseenalaistaa ja asiasta olla montaa eri mieltäkin. Kyseeseen tulee myös laitteen tunnistamisherkkyys. Kuinka tarkasti kuvien täytyy vastata toisiaan tunnistamisen takaamiseksi? Tähän olisi tietenkin helppo vastata, että 100 prosenttisesti. Mutta onko se ylipäänsä mahdollista saatikka sitten järkevää? Mikäli kasvojen täytyisi vastata koko passin voimassaoloajan täysin passissa olevaa kuvaa, mikä on kuvattu passin tilaamishetkeltä, ongelmat olisivat välittömästi edessä. Passin voimassaolo on enimmillään viisi vuotta ja viisi vuotta vanha kasvokuva äärimmäisen harvoin vastaa tuona aikana elämisen mukanaan tuomia muutoksia ihmisessä, joista helpoiten havaittavia ominaisuuksia ovat esimerkiksi hiukset, silmälasit ja parta; jopa onnettomuudet voivat aiheuttaa kasvoihin olennaisia muutoksia. Herääkin kysymys, onko kasvokuva oikea tunniste? Automaattista tarkastusta mainostetaan sillä, että se perustuu sellaisiin piirteisiin, jotka eivät muutu ja ovat yksilöllisiä. Haaste onkin oikean, vertailussa käytettävän ja hyväksyttävän yhtäläisyyden tarpeeksi suuren prosenttimäärän löytämisessä. Vastaus tarvitaan siihen, miten paljon kameran ottaman kuvan tulee vastata sirulla olevaa kuvaa. Liian alhainen yhdennäköisyysprosenttimäärä estää portin avautumisen laukaisevan kelpoisuuden täyttymisen. Toisaalta yhdennäköisyysprosenttimäärä ei voi olla taas liian korkea. Käytännössä on mahdoton ajatus, että kenenkään kuva vastaisi täysin sirulla olevaa vuosien takaista tai vaikka parin viikon takaistakaan kuvaa. Vaikkakin tunnistaminen perustuu pysyvinä pidettyihin piirteisiin, kuten silmien etäisyys toisistaa. Tämä aiheuttaisi vain sen, että suuri osa tunnistusyrityksistä tulisi hylättyinä takaisin. Kuvien täytyisi silloin vastata niin paljon toisiaan, ettei käytännössä kukaan vastaisi täysin sirul-

la olevaa kuvaansa. Biometriset tekijät ovat yksilöllisiä, mutta ehkä tekniikka ei ole vielä tarpeeksi kehittynyttä sen täysipainoiseen hyödyntämiseen.

Kolmas tavoite automatisoinnilla on henkilömäärään siirtäminen rajatarkastuksista muihin painopistealueen töihin. Nyt on Helsingissä koekäytössä kolmen portin linjasto. Tavoitteena olisi, että yksi rajavartija voisi hoitaa useita portteja yksin, kun perinteisessä rajatarkastuksessa jokaisella luukulla on yksi rajavartija tekemässä rajatarkastusta. Automatisoinnilla haetaan mahdollisuutta vähentää henkilömäärän vahvuutta yksinomaan rajatarkastusten tekemiseen. Koekäytössä oleva linjasto ei ole tähän mennessä juurikaan tuonut näitä tavoitteeksi asetettuja henkilömäärän vähennyksiä. Laitteiden toimintavirheiden virhesanomat sekä muiden käyttövirheiden selvitystyöt vaativat edelleen vähintään yhden, välillä useammankin, varmentajana toimivan rajavartijan työpanoksen täysin. Henkilöstön vähentämistavoitteiden saavuttamattomuus johtuu lisäksi osittain siksi, ettei passiautomaatteja käyttäviä matkustajia ole ollut vielä kovinkaan paljon. Biometrinen passi ei tunnu olevan vielä kovinkaan yleinen tai passiautomaattia ei muuten vain haluta käyttää. Kun biometriset passit tulivat vuoden 2006 elokuussa, aiheutti tämä uudistus suoranaisia ruuhkia poliisiasemilla kesällä passien myöntämisessä. Merkille pantavaa on se, että ihmiset eivät suinkaan hakeneet kilvan uutta passia, vaan vanhan 10 vuotta voimassa olevan halvemman passin, kun niitä vielä myönnettiin. Tämäkin osaltaan kertoo sen, että Euroopan mittakaavassa päästään automatisoinnissa kokonaisvaltaiselle tasolle aikaisintaan vuonna 2016, kun viimeisetkin vanhat passit poistuvat käytöstä.

Henkilömäärän vähennystavoitteisiin pyritään automatisoimalla rajatarkastuksia. Jos lasketaan, että rajavartijalla menee keskimääräin 30 sekuntia aikaa matkustajaa kohti, ja passiautomaatti kykenisi samaan kuin Australian SmartGate, eli 15 sekuntia matkustajaa kohden. Tällöin teoriassa automaatista menee kaksi matkustajaa samaan aikaan kuin rajavartijan luukulta. Edelleen, jos yksi rajavartija voisi toimia viiden passiautomaatin varmentajana ja jos meillä olisi kymmenen automaattia, tarvittaisiin kahden rajavartijan työpanos. Perinteisin menetelmin kymmenellä passiluukuilla tarkastusta suorittaisi kymmenen rajavartijaa. Seuraavassa taulukossa on havainnollistettu yksinkertaisin laskutoimituksin automatiikan mukana tuomia teoreettisia säästöjä:

	Automaattinen tarkastus	**Rajavartijan tarkastus**
portteja	10	10
matkustajia	10 000	10 000
matkustajia porttia kohden	1000	1000
keskimääräinen aika matkustajalla portilla	15 sekuntia	30 sekuntia
yhteenlaskettu aika jokaista porttia kohden	15 000 sekuntia	30 000 sekuntia
yhteenlaskettu aika jokaista porttia kohden	n. 4 tuntia 10 minuuttia	n. 8 tuntia 20 minuuttia
tarvittavien rajavartijoiden määrä	**2**	**10**
henkilötyötunnit	**n. 8 tuntia 20 minuuttia**	**n. 83 tuntia 20 minuuttia**

Osittain näihin edellä esitettyihin lukuihin perustuukin tavoitteet siirtyä automatisoituihin rajatarkastuksiin. Jossakin vaiheessa tulevaisuudessa Venäjästä tulee viisumivapaa maa, jolloin matkustajamäärän odotetaan kasvavan räjähdysmäisesti. Silloin itärajalla tarvitaan lisää voimavaroja rajatarkastuksiin ja rajavalvontaan. Toinen asia mihin halutaan siirtää voimavaroja, on kolmansien maiden kansalaisten rajatarkastukset. Lähtökohtaisesti rajavartioiden toimet pitäisi kohdentaa näihin asioihin, sillä Euroopan Unionin kansalaiset ovat pääsääntöisesti ”vähäongelmaisia”, eikä niitä pitäisi muutenkaan systemaattisesti tarkastaa kaikista rekistereistä Schengen-alueen vapaan liikkumisen vuoksi.

Saavutetaanko automatisoinnilla sitten nämä tavoitteeksi asetetut voimavarojen kohdennukset, jää nähtäväksi. Ainakaan tällä hetkellä automaattinen tarkastus ei näytä täyttävän toivottuja tavoitteita. Tälle on montakin selitystä. Järjestelmä on uusi koko maailmassa, eikä oikein missään muuallakaan ole sen parempaa tilannetta, kuin toisessakaan maassa. Tekniikka ei välttämättä ole vielä riittävällä tasolla, jotta järjestelmä olisi tarpeeksi luotettava kaikkien toimintojen automatisoinniksi. Eikä kaikkia toimintoja vielä voitaisikaan automatisoida, varsinkaan ennen kuin kaikki vanhat passit ovat käyttökelvottomia, eli vasta vuoden 2016 jälkeen. Tämänkin jälkeen pelkkään automatiikkaan luottaminen on kyseenalaista, koska kolmansissa maissa ei vielä ole, eikä kaikkiin maailman maihin voida olettaa tulevan vielä pitkään

aikaan automatiikan vaativaa biometristä passia. Kehitysmaiden valmiudet ja resurssit samaan biometrisen passin vaatimaan automatiikkaan eivät välttämättä ole samanlaiset kuin kehittyneiden maiden.

6. RAJATURVALLISUUDEN TULEVAISUUSNÄKYMIÄ

Kuten jo aikaisemmin todettiin, automatisoidut rajatarkastukset voivat Euroopan Unionin kansalaisten mittakaavassa tulla kokonaan operatiivisiksi aikaisintaan vuonna 2016 johtuen vanhoista kymmenen vuoden passeista, joista viimeisiä myönnettiin vielä vuonna 2006. Ainoastaan Euroopan Unionista tulevalla mahtikäskyllä voitaisiin kaikki kansalaiset velvoittaa hankkimaan biometriset passit ennen sitä. Tämä tulisi jäsenvaltioille kuitenkin suhteettoman kalliiksi, sillä uudet passit voisivat päätyä osittain tai jopa kokonaan valtioiden maksettaviksi; olisihan kohtuutonta vaatia kansalaisia hankkimaan uudet passit, vaikka entisten passien voimassaoloaika laillisesti olisi vielä voimassa. Kaikkia maailman maita ajatellen en usko täyden automatisoinnin tulevan kyseeseen vielä useisiin, jopa kymmeniin vuosiin. Euroopan Unionin kansalaiset ovat muutenkin vapaan liikkuvuuden piirissä ja painopiste rajatarkastusten onkin kohdentumassa kolmansien maiden kansalaisiin.

Automatisoitujen rajatarkastusten ja neliportaisen mallin mukaan rajaturvallisuus alkaa jo lähtömaissa viisumia hakiessa. Lähtömaihin tuleekin panostaa asettamalla sinne ammattitaitoista ja oikeilla järjestelmillä varustettua henkilöstöä käsittelemään viisumihakemuksia. Jo viisumia hakiessa tulee tehdä selvitys hakijan henkilöllisyydestä ja perusteluista hakea viisumia. Lähtömaihin tulee myös antaa koulutusapua ja teknistä tukea, jotta heidän omat viranomaisensa pystyisivät ottamaan enemmän vastuuta, ja ehkä jossain vaiheessa myös ottamaan biometriset passit käyttöön. Myös viisumeihin on aikomus aloittaa sormenjälkien käyttäminen tunnistamisen varmentamiseksi.

Kun rajatarkastuksia ei voi täysin automatisoida, täytyy henkilöstöä olla edelleenkin tekemässä perinteisiä rajatarkastuksia. Euroopan Unionin kansalaiset on kuitenkin mahdollista saada automatisoinnin piiriin. Automaattiset tarkastusportit tulisi saada niin luotettavalle tasolle, että vuonna 2016 ne voisivat hoitaa Euroopan unionin kansalaisten tarkastukset kokonaan. Tällöin ei tarvitsisi kuluttaa suuria henkilövaroja näihin tarkastuksiin ja suuremman osan tarkastusresursseista voisi kohdentaa kol-

mansien maiden kansalaisiin, missä tulevaisuuden painopistekin tulee olemaan. Laitteiden tulee lisäksi olla niin hyviä, että niiden voi luottaa tekevän tarkastukset sata, tai ainakin lähes sata prosenttisella varmuudella. Luotettavuudesta ei saisi olla pienintäkään epäilystä ja siksi tunnistuksen luotettavuutta voitaisiin parantaa ottamalla lisää biometrisiä tunnisteita kasvokuvan lisäksi. Euroopan Unioni edellyttää jäsenmaitaan lisäämään sormenjäljen passeihin viimeistään vuoden 2009 kesäkuussa. Sormenjälki tallennetaan biometrisen passin sirulle digitaalisesti, samoin kuten kasvokuva.

Tulevaisuudessa tavoitteena olisi siis saada rajatarkastuksia tekevän henkilöstön painopiste pois Euroopan Unionin kansalaisista kolmansien maiden kansalaisten tarkastuksiin. Tähänkin asiaan on todennäköisellä varmuudella tulossa jonkin asteista automatisointia tulevaisuudessa. Automatisointi voi olla esimerkiksi rajavartijan tekemän maahantulopuhuttelun korvaaminen automaattisella laitteella. Tällaisen tavoitteen uskoisin kuitenkin olevan melko haasteellinen, sillä mielestäni on perusteltua kyseenalaistaa laitteen paremmuus tekemään maahantulotarkastusta verrattuna kokeneeseen rajavartijaan, joka useiden vuosien työkokemuksen perusteella osaa poimia (niin sanotusti haistaa) epäilyttävät tapaukset tarkempaan tarkastukseen. Biometriset asiakirjat pitäisi saada niin hyvälle tasolle, ettei niiden väärentäminen ole mahdollista tai että väärä henkilö pystyisi niitä käyttämään. Samoin automaattisten tunnistimien tulisi olla sata prosenttisen luotettavia. Automatisoitujen rajatarkastusten yksi perusidea on, kun tekniikka sen vain sallii, että rajatarkastus tehtäisiin jo ennen henkilön saapumista kohdemaan rajatarkastukseen. Tällöin tarvitsee olla ehdottoman varma tunnistus henkilöstä viisumia myönnettäessä, ja kun henkilö astuu lentokoneeseen, sillä rajatarkastus kaikkia mahdollisia rekistereitä hyväksi käyttäen tehdään jo lentokoneen ollessa vielä ilmassa. Kohdemaassa puolestaan tulisi olla niin hyvät automaattiset portit, että tieto epäilyttävistä henkilöistä on edennyt ennen heitä porteille asti, jolloin ne eivät päästä tällaisia tapauksia läpi. Tässä yhteydessä herää kysymys, kuka määrittelee sellaisen ominaisuuksien rajan, jonka ylitettyään henkilö on epäilyttävä? Voisiko epäilyttävyyden määrittely liittyä henkilön elämänkatsomukseen, poliittisiin mielipiteisiin vai riittäisikö tällaiseksi syyksi tuomiot tietyistä rikoksista?

Laitteiden kehittäminen on koko ajan käynnissä ja eri puolilla maapalloa testataan parhaiten omiin olosuhteisiin soveltuvia laitteita. Kehityksessä olisi kuitenkin hyvä tehdä edes jossain määrin kansainvälistä yhteistyötä. Ei ole kovinkaan järkevää, että

on olemassa monta erilaista ja monta lähes samanlaista järjestelmää, kuten merkiksi on LCD-televisioissa. Yhteistyötä tekemällä pystyttäisiin ottamaan huomioon jo järjestelmän kehittelyvaiheessa mahdolliset osapuolten erilaiset ominaispiirteet ja erikoistoiveet, tekemään kompromisseja ja siten saavuttamaan mahdollisimman yhtenäinen järjestelmä mahdollisimman monen maan käyttöön helpottamaan ja varmistamaan koko Schengen-alueen yhteistä turvallisuutta. Yhteistyöllä myös pystyttäisiin kehittämään tätä järjestelmää mahdollisimman taloudellisesti ja kustannustehokkaasti, koska mahdolliset järjestelmän toimintavirheet pystyttäisiin nopeasti havaitsemaan ja hakemaan muita ratkaisuja näiden korjaamiseksi ajoissa. Jokaisen maan oma itsenäinen kehitystyö aiheuttaa luonnollisesti toisistaan poikkeavia järjestelmiä. Jos Schengen-alueella jonkun maan järjestelmän toimivuus on heikommalla tasolla kuin muiden, muodostuu tämä yhden maan ongelma nopeasti koko Schengen-alueen ongelmaksi.

Schengen-alueella ihmisten vapaa liikkuminen helpottaa kansalaisten liikkumista, mutta samalla se helpottaa myös rikollisten mahdollisuutta vapaaseen liikkumiseen maasta toiseen. Koko Schengen-alueen ulkorajan, mitä Suomikin on osa, tulee erityisesti panostaa rajaturvallisuuteen. Lentokentät ovat tavallaan tärkeämmässä roolissa, kuin maarajat. Lentokentille saavutaan kauempaa ja useammista maista kuin maarajalle. Suuri osa Suomeenkin tulevista turvapaikan hakijoista saapuu lentokoneilla, Irakista ja Somaliasta [27]. Maarajojen kautta maahan tulee muitakin kuin vain naapurivaltion kansalaisia, mutta harvemmin kauempaa kolmansien maiden kansalaisia, jotka yleensä tulevat kauempaa. Osa turvapaikan hakijoista on jopa turvautunut ammattimaiseen ihmissalakuljetukseen ja saattavat tulla jopa Irakista asti piiloutuneena rekkoihin tai laivoihin. Tosin tällaisin keinoin maahan saapuneiden turvapaikan hakijoiden kertomuksiin matkan tapahtumista, järjestelyistä tai matkaan johtaneista syistä kannatta suhtautua varauksella [28].

Tulevaisuudessa myös pohdittavaksi nousee kysymys, kuinka järjestää lentoaseman yleisten tilojen valvonta ja voisiko sitä automatisoida. Suurilla lentokentillä matkaa lentokoneelta matkalaukkujen vastaanottoon ja sieltä rajatarkastukseen voi olla satoja metrejä. Tällä välialueella on mahdollista tapahtua mitä vaan. Riittävätkö yleisiä alueita valvomaan pelkästään kävelevät partiot, vai tarvitaanko kenties lisäykseksi automaattista valvontaa? Entä riittäisikö pelkästään kameravalvonta? Jatkuva kameravalvonta kysyy henkilöresursseja kuvaruudun ääressä ja onko heillä kykyä havainnoida kaikkea saatikka vaikuttaa havaittuihin tapauksiin. Tulevaisuudessa uskoi-

sin kaikenlaisten tunnisteiden lisääntyvän myös yleisiin aulatiloihin, esimerkiksi kasvojentunnistin-ohjelma voisi olla ensimmäisten joukossa, mutta myös kaikenlaisten röntgen-, infrapuna- ja vaarallisten aineiden tunnistimien voi olettaa lisääntyvän. Aikataulua tällaisille tunnistimille on tässä vaiheessa vaikea ennustaa.

7. JOHTOPÄÄTÖKSET

Automatisoidut rajatarkastukset ovat uuden tekniikan hyödyntämistä rajatarkastuksissa muutenkin, kuin pelkän passin tarkastamiseksi. Suomessa automatisoidut rajatarkastukset ovat vasta suunnittelu-, kehittely ja kokeiluasteella. Tämä tutkimus onkin tehty selventämään, mitä ne luultavimmin tulevat olemaan tai ainakin millaisia niiden pitäisi olla. Yhdysvalloissa on jo jossain määrin käytössä Smart Border -niminen automatisoitu rajatarkastusmenetelmä, jonka kolme peruspilaria on seulonta, biometriikka ja informaatioteknologia.

Tutkimuksen perusteella automatisoitujen rajatarkastusten tärkein saavutus Rajavartiolaitoksen kannalta on ehdottomasti rajaturvallisuuden parantuminen ja tämä on tärkein syy, miksi siihen tullaan siirtymään. Myönteistä on myös rajatarkastusten nopeutuminen ja helpottuminen. Rajaturvallisuus on kuitenkin muutakin, kuin pelkkä rajaviivan turvallisuus. Rajaturvallisuus vaikuttaa oleellisena osana myös sisämaassa vallitsevaan yleiseen järjestykseen ja turvallisuuteen.

Biometristen passien ja tunnistimien käyttäminen 4-portaisen rajavartiomallin yhteydessä selkeyttää maahantulijoiden valvontaa. Oikealla henkilöllä on aina oikeista syistä myönnetty viisumi. Biometrisella passilla henkilöllisyyden toteaminen lähtömaassa on luotettavaa, sillä biometriset tunnisteet ovat tämänhetkisellä tekniikalla luotettavimpia yksilökohtaisia tunnisteita. Henkilön tunnistaminen rajatarkastuksen yhteydessä on luotettavaa ja saadaan täysi varmuus siitä, että rajatarkastuksessa oleva henkilö on juuri se henkilö, jolle lähtömaassa myönnettiin viisumi oikeilla perusteilla. Biometrisen tunnistamisen voi hoitaa automaattisesti erilaisilla tunnistinlaitteilla, eikä siihen tarvitse käyttää niin paljoa henkilöstöresursseja, kuin tämänhetkisellä rajatarkastusmenetelmällä. Tämä helpottaa rajavartijoiden työtä, sillä tällä hetkellä rajatarkastusta tekevä rajavartija tutkii henkilökohtaisesti matkustusasiakirjan aitouden suurennuslasilla ja UV-valolla. Aitouden toteamisen jälkeen rajavartija yrittää selvittää onko henkilö passin henkilö. Keinot henkilöllisyyden varmentamiseksi

ovat tällä hetkellä aidoksi todetun passin kuvan vertaaminen passia esittävään henkilöön ja maahantulopuhuttelu. Biometriset passit ovat myös huomattavasti vaikeampia väärentää kuin perinteiset passit, joten rajavartijoiden resursseja ei käytetä turhaan passien aitouksien toteamisiin. Matkustajamäärien jatkuvasti lisääntyessä vähemmillä henkilöstöresursseilla toimivat tehokkaammat automaattiset tarkastusportit ovat tervetulleita.

Tavallisen matkustajan ja rajanylittäjän kannalta suurin hyöty on rajatarkastusten nopeutuminen. Matkustusaika lyhenee, kun ei tarvitse kuluttaa aikaa rajatarkastuksissa ja jonoissa. Jotkut matkustajat voivat tosin kokea automatisoidut rajatarkastukset yksityisyyden menettämisenä ja häiritsevänä ”isoveli valvoo” -sjärjestelmänä. Sitä se ei kuitenkaan ole. Automatisoituihin rajatarkastuksiin tulee asennoitua meidän jokaisen turvallisuutta parantavana systeeminä. Emme saa tuudittautua käsitykseen, että elämme kaukana maailman pahuudesta omassa viattomassa lintukodossa, jossa kaikki ovat turvassa. Maailmassa on valitettavan paljon ihmisiä, joille riittää perusteluksi aiheuttaa tuhoa ja hävitystä muulle maailmalle ainoastaan vääräuskoisuudesta syyttämisellä. Valtion tehtävänä on suojella omia kansalaisiaan mahdollisilta suuronnettomuuksilta ja joukkotragedioilta. Vaikka kansalaisten valvonta tuntuisikin ehkä yksityisyyden rajoittamiselta, on ymmärrettävä suurempia kokonaisuuksia. On pidettävä mielessä, että rajojen avoimina pitäminen ilman, että kukaan valvoo mahdollistaa myös terroristien vapaan liikkumisen ja vaivattoman väylän terroriteoille.

Tällä hetkellä uusia Helsinki-Vantaan lentoasemalla koekäytössä olevia passiautomaatteja käytetään harmittavan vähän, eikä käyttöön perustuvia kokemuksia ole sen vuoksi vielä paljoa. Tämä osaltaan johtunee siitä, ettei kovinkaan monella ole vielä käytössään biometrista passia. Biometristen passien puute voi myös olla omiaan muodostamaan käsitystä koko automatisoinnin tarpeellisuudesta yleensä. Lisäksi ne matkustajat, jotka ovat käyttäneet passiautomaatteja, ovat saattaneet kokea laitteet epäkäytännöllisiksi ja aikaa vieviksi, joihin on voinut olla syynä yksinkertaisesti se, ettei ole riittävästi huomioitu laitteiden erittäin tarkkoja toimintaohjeita. Kesäkuussa 2009 tuleva uudistus sormenjäljen lisäämisestä biometriseen passiin voi seuraavaksi antaa biometriikan vastustajille uutta puhtia; ensin piti antaa kasvokuva passiin ja nyt pitäisi antaa jo sormenjälkikin. Seuraavaksi pitää varmaan antaa jo DNA-näyte.

Tähän tutkielmaan ei ole kuulunut kyselytutkimusta, joten edellä kuvatut tuntemukset ovat omia olettamuksiani mahdollisista eteen tulevista todennäköisistä teista perustuen lähdeaineistosta saamaani kuvaan sekä yleistuntumaan, että jokaiseen uuteen asiaan liittyy niin puolestapuhujia kuin monen tasoisia vastustajiakin. Kartoittamalla etukäteen mahdollisimman laajasti järjestelmän tehokasta toimintaa haittaavat tekijät edesautetaan uuden järjestelmän sisäänajoa ja vähennetään mahdollista matkustajien taholta esiintyvää vastustusta. Automatisoiduissa rajatarkastuksissa tulisikin ymmärtää projektin pitkäjänteisyys. Kun aletaan kehittää täysin uutta järjestelmää, johon ei vielä ole edes kaikkea tekniikkaa olemassa, on varauduttava siihen, että siihen kuluu todella paljon aikaa. Asiat eivät tapahdu sormia napsauttamalla, vaan joudutaan kokeilemaan paljon erilaisia järjestelmiä, jotta tiedetään mikä soveltuisi parhaiten ja mihin suuntaan tekniikan kehitystä pitäisi viedä.

Tällä hetkellä olemassa oleva tekniikka ei välttämättä ole oikea automaattisiin rajatarkastuksiin. Laitteita tulisi kehittää vielä huomattavan paljon enemmän, jotta niiden voisi luottaa hoitavan itsenäisesti ja automaattisesti rajatarkastukset. Luottamus järjestelmän toimivuuteen on tärkeää, sillä epäluottamus syö nopeasti rajavartijoiden työmotivaatiota. Kun laitteita ja järjestelmiä kehitellään, on tärkeää myös ottaa huomioon rajatarkastuksia tekevien työntekijöiden mielipiteitä, koska juuri heillä on käytännön tuntuma ja kokemus näihin tehtäviin. Mikäli automaattisten porttien linjaston varmentajana toimiva rajavartija kokee laitteen epäluotettavaksi, niin ajan mittaan turhautumisen riski kasvaa. Rajavartijan ”tee työtä jolla on tarkoitus” - ideologia omasta työstä tilanteessa, jossa automaatin toimintavarmuus on kyseenalainen, ymmärrettävästi voi kärsiä alennustilaa, jos ilman laitteita tehtäessä tarkastus olisi huolellista ja tehty sataprosenttisella teholla. Siksi automaattien kehitystyön merkitystä saada niistä täysin luotettavia, ei voi väheksyä. Automaattien kehitystyötä tehdään koko ajan ja tuloksia koekäytöistä analysoidaan sitä mukaa, kun niitä tulee.

Sisämaassa ei välttämättä tiedetä, mitä Rajavartiolaitoksen tekee, toisin kuin rajan läheisyydessä sijaitsevissa kunnissa. Hyvänä esimerkkinä tästä tiedon puutteesta voi tulkita 18.2.2009 Kuopion Kaupunkilehdessä ilmestyneestä Rajavartiolaitoksen rekrytointi-ilmoituksesta, jossa haettiin rajavartijaa Kaakkois-Suomen Rajavartiostoon. Ilmoitus oli mitäänsanomattoman pieni, eikä siinä ollut kuvaa tai muuta katseenvangitsijaa lisäämässä rajavartijan työn houkuttavuutta. Ilmoituksen pienellä tekstillä kehotettiin lukijaa menemään Rajavartiolaitoksen Internet-sivuille hankkimaan lisätietoja. Mielestäni Rajavartiolaitoksen tulisi tehdä eräänlainen kasvojenko-

hotus mediassa ja tuoda Rajavartiolaitoksen ensiarvoisen tärkeä tehtävä laisten turvallisuuden lisääjänä ihmisten tietoisuuteen paremmin. MTV3:n uutisissa uutisoitiin 18.10.2007 poliisin ja Rajavartioston tutkivan paritusasiaa. Tämä varmaan pitääkin paikkansa muilta osin, paitsi että viranomainen on Rajavartiolaitos, joka tutkii tapausta yhteistyössä poliisin kanssa. Mikäli uudet passit markkinoidaan vain parempana tunnistuskeinona, ihmisille voi jäädä väärä kuva Rajavartiolaitoksesta kansalaisten kyttääjänä. Kansalaisille tulisi tehdä selväksi perusteet miksi halutaan siirtyä automatisoituihin rajatarkastuksiin ja mitä se käytännössä tarkoittaa. Ei ole kyse kansalaisten valvomisesta, vaan kotimaan pitämisenä turvallisena kansalaisille. Suomi on pysynyt muita maita turvallisempana paitsi sijaintinsa vuoksi, myös Rajavartiolaitoksen tehokkaan toiminnan ansiosta. Rajavartiolaitokselle on taattava mahdollisuus pystyä turvaamaan kansalaisten turvallisuus tulevaisuudessakin ja varattava mahdollisuus hyödyntää kaikkia niitä menetelmiä, joilla tähän tavoitteeseen päästään.

LÄHTEET

[1] Ackleson, Jason; Border Security Technologies: Local and Regional Implications. Review of Policy Research, Volume 22, Number 2 (2005)

[2] Action Plan for Creating a Secure and Smart Border. Office of Homeland Security. December 12, 2001.

[3] Andreas, Peter; Border security in the age of globalization: How can we protect ourselves without losing the benefits of openess? Regional Review; 2003 3rd Quarter, Vol. 13 Issue 3, p3-7, 5p, 4c.

[4] Eskola, Antti; Sosiologian tutkimusmenetelmät. WSOY:n graafiset laitokset. 1981

[5] Hirsijärvi, Sirkka – Remes, Pirkko – Sajavaara, Paula; Tutki ja kirjoita. Tammer-Paino Oy. 1997.

[6] http://217.71.145.20/TRIPviewer/temp/TUNNISTE_U_26_2004_fi.html [Valtioneuvoston kirjelmä Eduskunnalle ehdotuksesta neuvoston asetukseksi EU:n kansalaisten passien turvatekijöitä ja biometriikkaa koskevista vaatimuksista (passiasetus)]

[7] http://ec.europa.eu/news/justice/071221_1_fi.htm

[8] http://en.wikipedia.org/wiki/Computer_reservations_system

[9] http://eur-lex.europa.eu/LexUriServ/site/fi/com/2004/com2004_0116fi01.doc

[10] http://fi.wikipedia.org/wiki/Biometrinen_tunnistaminen

[11] http://fi.wikipedia.org/wiki/Tiedosto:Schengenzone.svg

[12] http://pdf.directindustry.com/pdf/automatic-systems/security-booth-sng-770-series/16325-36093-_8.html [Direct Industry laitevalmistajan sivut]

[13]http://raja.fi/rvl/bulletin.nsf/HeadlinesPublicFin/C7AC8FFD6C86A01DC225751B0032A973

[14]http://raja.fi/rvl/home.nsf/pages/948FD75BD92B69D0C225747F00461D84?Opendocument

[15] http://zing.ncsl.nist.gov/biousa/html/workshop08.html The International Workshop on Usability and Biometrics – konferenssissa Jean-Christophe Fondeurin esitelmä Usability of Biometrics for Border Crossing

[16] http://zing.ncsl.nist.gov/biousa/html/workshop08.html, The International Workshop on Usability and Biometrics – konferenssissa Mario Sibucaon esitelmä Biometrics at the Philippine Social Security System

[17] http://www.customs.gov.au/site/page.cfm?u=5831 [Australian Customs Service -sivut]

[18]http://www.customs.gov.au/webdata/resources/files/protecting_our_borders1.pdf [Australian Customs Service - sivut]

[19] http://www.digitoday.fi/tietoturva/2008/10/02/elviksen-passi-kelpasi-lentokentalla--katso-video/200825717/66

[20]http://www.digitoday.fi/yhteiskunta/2008/08/06/biopassin-murtaminen-onnistui-tutkijalta-nopeasti/200820308/66

[21] http://www.helsinki-vantaa.fi/hel_tiedote?id=71873

[22] http://www.hs.fi/extrat/erikoissivu/1101980148333

[23]http://www.hs.fi/ulkomaat/artikkeli/Kohutaitelija+Vilks+painui+maan+alle/1135230372521

[24] http://www.ier.fr/~/uk/market/access-control/~/uk/focus_on/air-france-is-testing-the-pegase-project/index.html [Turvallisuuslaitteita valmistavan IER -yhtiön sivut]

[25] http://www.iltalehti.fi/ulkomaat/200812188793498_ul.shtml

[26]http://www.intermin.fi/intermin/hankkeet/biometria/home.nsf/pages/4BB93202E6BDC28AC225701C004319D4?opendocument.

[27] http://www.migri.fi/netcomm/content.asp?path=8,2709,2717,2731

[28] http://www.mtv3.fi/uutiset/arkisto.shtml/arkistot/kotimaa/2009/02/802713

[29] http://www.ukba.homeoffice.gov.uk/managingborders/technology/iris/ [UK Border Agencyn sivut]

[30]http://www.ukba.homeoffice.gov.uk/sitecontent/documents/managingourborders/eborders/irisdownloads/irisarrivalguide.pdf

[31] Niemenkari, Arto: Rajaturvalllisuus Euroopan Unionissa. Raja- ja merivartiokoulun julkaisusarja 1. Tutkimuksia nro 1 2003. s 38.

[32] Rajavartiolaki (578/2005).

[33] Zureik, Elia - Salter, Mark B.: Global Surveillance and Policing: Borders, security, identity. Willan Publishing, Devon 2005. Chapter 8 s. 113 - 138.

[34] Marttinen, Pasi. Virolahden rajavartioalueen päällikkö majuri Pasi Marttisen esittelyluento Virolahden rajavartioalueesta kadeteille 11.9.2007 Virolahden rajavartioalueen johtopaikalla.

[35] Tiainen, Janne. Tiedot automatisoinneista käytännössä ja niiden kehitysideoista Helsinki-Vantaan lentoasemalla perustuvat Helsingin Rajatarkastusosaston luutnantti Janne Tiaisen haastatteluun tammikuussa 2009. Haastattelumateriaali tutkijan hallussa.