jamk.fi

Kuljetus- ja logistiikkaketjujen kyber-turvallisuus, uhat ja merkitys yrityk-sille

Otto Harju

Opinnäytetyö
Toukokuu 2021
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), Tieto- ja viestintätekniikka

Information and communication technologies
Bachelor's Degree Programme in Information and Communications Tech-nology

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Harju, Otto	Opinnäytetyö, AMK	Toukokuu 2021
	Sivumäärä 58	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: Kyllä

Työn nimi

Kuljetus- ja logistiikkaketjujen kyberturvallisuus, uhat ja merkitys yrityksille

Tutkinto-ohjelma

Insinööri (AMK), tieto- ja viestintätekniikka

Työn ohjaaja(t)

Rantonen Mika

Toimeksiantaja(t)

Vatanen Marko / JYVSECTEC

Tiivistelmä

Teknologian kehittyminen näkyy haastavana ilmiönä kyberturvallisuuden keskuudessa. Kuljetussektorin kasvava teknisten järjestelmien määrä muun muassa raskaan kuljetuskaluston käytössä altistaa entistä enemmän kuljetus- ja logistiikkaketjuja kyberhyökkäyksille.

Opinnäytetyö toteutettiin JYVSECTEC:n toimeksiannosta ja sen tavoitteena oli selvittää kuljetus- ja logistiikkayrityksien kyberturvallisuuden merkitystä sekä uhkia yrityksille.

Tutkimuskysymyksinä oli selvittää kuljetus- ja logistiikkaketjuihin kohdistuvia kyberuhkia, miten kuljetus- ja logistiikkaketjujen kyberuhkia pystytään välttämään sekä kyberturvallisuuden merkitys yrityksille. Ratkaisuja ei toteutettu käytännössä vaan pyrittiin kokonaisvaltaiseen tutkimukseen, joka hyödyttää kuljetus- ja logistiikkasektoria ja kyberturvallisuuden alaa. Tutkimusmenetelmäksi valikoitui edellä mainitun perusteella laadullinen eli kvalitatiivinen tutkimusmenetelmä.

Opinnäytetyössä tarkasteltiin kuljetus- ja logistiikkaketjuja ja niihin liittyviä riskejä ja poikkeamia, joihin mahdollisesti voitaisiin vaikuttaa haitallisesti. Työssä keskityttiin logistiikan historiaan, nykyajan rakenteeseen, toimitusketjuun sekä sen tietojärjestelmiin. Muita käsiteltäviä aiheita olivat kuljetus- ja logistiikkaketjujen kyberturvallisuus sekä niihin kohdistuneet hyökkäykset ja digitaalisen turvallisuuden parantamiseen liittyvät edellytykset.

Tuloksien perusteella kuljetus- ja logistiikkaketjujen tulee kiinnittää huomiota teknisten järjestelmiensä ja tietoverkkojensa turvallisuuteen nyt sekä tulevaisuudessa. Merkittävinä pidettäviä kehityskohteita ovat yritysten kyberturvallisuusstrategian kehittäminen, tietoturvapoikkeumien havainnointi sekä kuljetuskaluston teknisten järjestelmien turvaaminen.

Avainsanat (asiasanat)

kuljetus- ja logistiikkaketjut, digitaalinen turvallisuus, kyberuhat

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Harju, Otto	Bachelor's thesis	May 2021
		Language of publication: Finnish
	Number of pages: 58	Permission for web publication: Yes

Title of publication

Cyber security of transport and logistics chains, threats and importance for companies

Degree programme

Bachelor's Degree Programme in Information and Communications Technology

Supervisor(s)

Rantonen Mika

Assigned by

Vatanen Marko / JYVSECTEC

Abstract

The development of technology occurs as a challenging phenomenon among cyber security. Rising number of technical systems in the transport sector for example in the use of heavy transport is increasingly exposing transport and logistics chains to cyber-attacks.

This thesis was carried out on the mandate of JYVSECTEC and was aimed at finding the importance of cyber security for transport and logistics companies and threats to businesses.

Research questions were to find out cyber threats regarding transport and logistics chains, how to avoid cyber threats in transport and logistics chains and the importance of cyber security for companies. Solutions were not implemented in practice but sought for a comprehensive research that benefits the transport and logistics sector and cyber security field. The research method was selected based on the aforementioned reasons to be the qualitative method of research.

The thesis examined transport and logistics chains and related risks and deviations that may be adversely affected and focused on the history of logistics, modern structure of logistics and supply chain and its information systems. Other subjects to be addressed were cyber security of transport and logistics systems and attacks carried out towards them as well as requirements for improving digital safety.

Based on the results, transport and logistics chains should pay more attention to the safety of their technical systems and data networks both now and in the future. Significant development areas include development of corporate cybersecurity strategy, detection of security breaches and securing the technical systems of transport equipment.

Keywords/tags (subjects)

transport and logistics chains, digital security, cyber threats

Miscellaneous (Confidential information]

Sisältö

Kuviot

Taulukot

Lyhenteet

AEI	Automatic equipment identification
BIOS	Basic Input Outboot System
CAN	Controller Area Network
CCEOP	Cold Chain Equipment Optimization Platform
EAN	International Article Number
EDI	Electronic Data Interchange
GNSS	Global Navigation System
GPS	Global Positioning System
GSM	Global System for Mobile communication
HA	High Accuracy Service
HTML	Hypertext Markup Language
IoT	Internet Of Things
MBR	Master Boot Record
MEOSAR	Medium Earth Orbiting Search and Rescue
NSA	National Security Agency
OCR	Optical Character Recognition
PRS	Public Regulated Service
RFID	Radio Frequency Identification
SMB	Server Message Block
XML	Extensible Markup Language

1 Johdanto

Opinnäytetyön tavoitteena on tutkia sekä tuoda ilmi erilaisia uhkakuvia ja toimintojen merkityksiä, jotka liittyvät logistiikkajärjestelmien kyberturvallisuuteen yleisesti yritysten osalta. Opinnäytetyössä käsitellään logistiikkaketjujen käytössä olevia tietojärjestelmiä ja niiden turvallisuutta, jonka lisäksi keskitytään kuljetus- ja logistiikkaketjujen uhkakuvien vertailuun ja tutkintaan.

Tietojärjestelmien jatkuva kasvu yhteiskunnassa vaatii turvallisuusjärjestelmien toistuvaa päivitystä ja huolenpitoa. Nykyajan moderni liikemaailma on toteutettu lähes kokonaan teknologisesti ja kaikki toiminnot ovat liitetty toisiinsa. Tämä tekee koko järjestelmästä yhtenäisen verkkoon kytketyn kokonaisuuden. Kaikki toiminta liikemaailmassa on yhdistetty tietojärjestelmien ympärille ja on täten saatavilla kellon ympäri. Ongelmana teknologisessa kehityksessä on rikollisuuden kehittyminen samalla tahdilla. Yritykset joutuvat varautumaan entistä enemmän kyberrikollisuuteen ja sen tuomiin haasteisiin. Vuodesta 2016 lähtien Yhdysvalloissa on tapahtunut päivittäin yli 4000 kiristyshaittaohjelmaa tarkoittaen 300 prosentin kasvua edellisestä vuodesta. Kyseisten lukujen varjossa huomataan kehittyneiden kyberturvallisuustoimintojen tärkeys, jotka pitäisivät olla samassa, ellei tärkeämmässä kehityskaaressa yritysten fyysisten turvallisuusjärjestelyiden kanssa. (Churchill 2018.)

Vaikka digitaalinen muutos ja automaation kehittyminen ovat osoittautuneet olevan kasvavassa roolissa kuljetus- ja logistiikkasektorilla, niiden kehitys on mahdollistanut sektorin olevan yhä suuremmassa vaarassa erilaisten kybervaikuttamisten -ja hyökkäyksien suhteen. Kun yhä useampaa toimitusketjun haaraa aletaan siirtämään pilvipalveluihin, avaa tämä yhä useamman mahdollisuuden uhkatekijälle päästä käsiksi tietoihin, jotka ovat salattuja. (Cybersecurity for transport and logistics industry 2020.)

Opinnäytetyön toimeksiantajana toimi Jyväskylä Security Technology (JYVSECTEC). JYVSECTEC on Suomen johtava kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus, joka toimii osana Jyväskylän ammattikorkeakoulun tieto- ja viestintätekniikan instituuttia. Yhteistyö IT-instituutin kanssa takaa monipuolisen asiantuntijaverkoston

ja laajan asiantuntemuksen muun muassa kyberturvallisuudesta, reagoimisesta tietoturvapoikkeamiin, kehittyvistä teknologioista ja IT-teknologioista. JYVSECTEC pyrkii toiminnallaan vahvistamaan teknologista kehitystä ja valmiutta nykyaikaisiin uhkiin, sekä tuottamaan asiakkailleen arvokasta palvelua muun muassa kyberturvallisuusharjoitusten, henkilöstökoulutuksen, ohjelmistotestauksen, konsultointipalveluiden sekä akkreditointi- ja sertifiointitoimintojen muodossa. (Overview n.d.)

2 Tutkimusasetelma

2.1 Tutkimuskysymykset

- Millaisia kyberuhkia kuljetus- ja logistiikkaketjuihin kohdistuu?
- Miten kuljetus- ja logistiikkaketjuihin liittyviä kyberuhkia voidaan välttää?
- Mikä merkitys kyberturvallisuudella on yrityksille?

2.2 Tutkimusmenetelmät

Työn tarkoituksena oli tutkia kyberturvallisuuden kokonaiskuvaa kuljetus- ja logistiikkaketjuissa ja vastata erityisesti edellisessä kappaleessa esitettyihin tutkimuskysymyksiin. Opinnäytetyössä hyödynnetään tutkimusotteena laadullista eli kvalitatiivista tutkimustapaa. Kvalitatiivisessa tutkimuksessa tavoitteena on ymmärtää kohteen laatua, ominaisuuksia ja merkitystä kokonaisuudessaan. Aineistoa kerätään useista lähteistä, joiden perusteella pyritään tekemään johtopäätöksiä kokonaisuuden muodostamiseksi. Laadullisen tutkimuksen menetelmissä korostuvia näkökulmia ovat esimerkiksi ilmiön esiintymisympäristö, tausta, merkitys ja ilmaisu. Laadullinen tutkimus pyrkii tuottamaan yksityiskohtaista sekä monipuolista tietoa tutkittavasta ilmiöstä. (Laadullinen tutkimus 2015.)

2.3 Tutkimuksen luotettavuus

Työn teoriaosuus pohjautuu logistiikkaan ja kyberturvallisuuteen liittyvään kirjallisuuteen, blogikirjoituksiin sekä valtiotason ja asiantuntijoiden julkaisuihin aiheista. Tutkimuksesta johdettu tulos on tavoitteellinen ja siihen pääsemiseksi on hyödynnetty monia eri aineistotyyppejä ja analyysimenetelmiä. Työssä arvioidaan tutkimuksen uskottavuutta ja luotettavuutta, joiden perusteella voidaan päätellä tutkimuksen tuloksien olevan yleistettävissä muiden toimialojen menettelyiden kanssa. (Tutkimuksen toteuttaminen 2010.)

3 Logistiikan merkitys

3.1 Logistiikan alkulähteillä

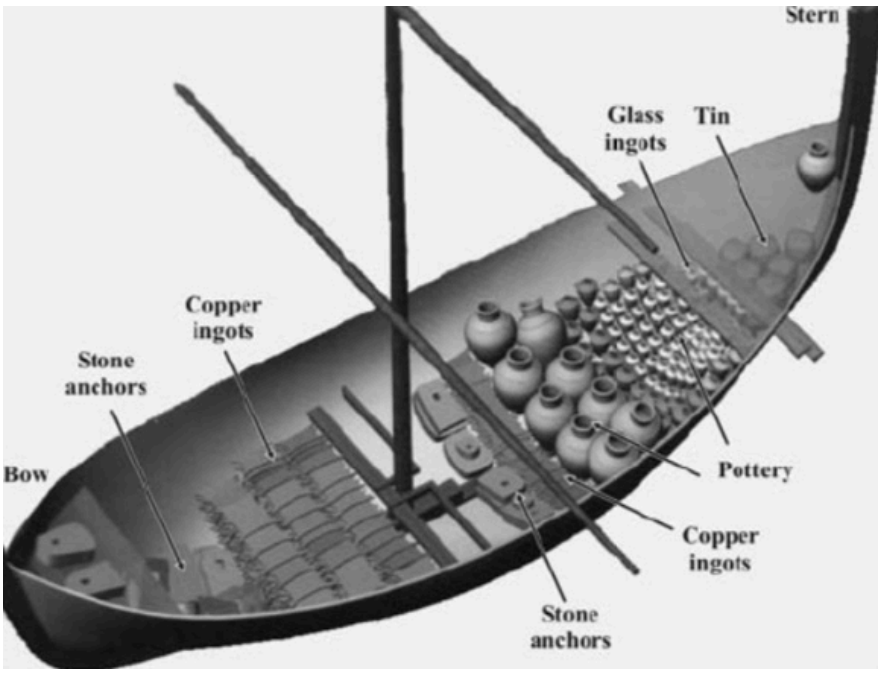
”Suppeassa merkityksessä logistiikalla tarkoitetaan vain tavaroiden kuljetusta ja varastointia. Laajassa merkityksessä logistiikka on materiaali-, raha- ja tietovirtojen hallintaa.” (Mitä on logistiikka? n.d.)

Muinaisessa historiassa logistiset tarpeet rinnastettiin pääosin asevoimien toimintoihin ja sodankäyntiin, mutta logistiikkaan verrattava suunnittelu on alun perin lähtenyt liikkeelle kaupunkien infrastruktuurin luomisesta ja kehittämisestä. Neoliittisen ajanjakson (6000–3500 *eaa*.) aikana Afrikan ja Aasian suurten jokien – Niilin, Tigrisin ja Eufratin – varsille alkoi ilmestyä yhteisöllisiä ja yhteiskunnallisia rakennelmia, jotka pitivät sisällään edistyksellistä järjestelyä, kaavoitusta ja suunnittelua. Tämän episteemisen perustan syntyminen on edelleen yksi suurin keskustelunaihe ihmisen piirteitä ja kulttuuria tutkivan antropologian parissa. Aikaisimmat historialliset kirjoitukset logistiikan toiminnasta ikuisti kuuluisa kreikkalainen matemaatikko ja filosofi Pythagoras (582–496 *eaa*.). Hän oppi logistiikan ja geometrian taitoja muun muassa foinikialaisilta, joiden avulla Pythagoras mahdollisti nimittämisensä logistikoksi. (Stojić, Tanackov & Tepić 2011.) Kun muinaiset Rooman, Egyptin ja Kreikan armeijat valloittivat antiikin aikoina (800 *eaa*. – 500 *jaa*.) heidän silloiset alueensa, käyttivät he

sotilastaktiikoita, jotka olivat ennenäkemättömiä silloisessa maailmankuvassa. Näissä taktiikoissa korostui erityisesti tarvikkeiden kuljetusvarmuus. Erityisen maineikkaita toiminnassaan olivat Rooman valtakunnan armeijan perusyksiköt, legioonat. (How logistics began 2019.) Rooman armeijan alkuaikoina rivisotilaan oletettiin hankkivan itse tarvittavat välineet ja ravinto itselleen, mutta ajan kuluessa armeija siirtyi lähes kokonaan valtion tukemaksi sotajoukoksi. Valtavan ravinnontarpeen lisäksi armeija tarvitsi haarniskoita, aseita, lääkintätarvikkeita, sekä rakennusmateriaaleja. Rooman valtakunnan tuli varmistaa sotajoukkojensa varusteiden ja ravinnon saanti, vaikka he olivat valloittamassa tuhansien kilometrien päässä. 215 *jaa.* sotajoukot komentajineen olivat Espanjassa ja ilmoittivat Rooman neuvoa antavalle neuvostolle, senaatille, heidän tarvikepuutteestaan. Vajetta oli muun muassa rahasta, jota armeija päätti hankkia paikallisia verottamalla, mutta ravinto ja vaatetus täytyi kuljettaa Italiasta asti. Senaatille tämä ei ollut ongelma ja tarvittava maissi rahdattiin Italiasta Espanjaan. Yksityisiä toimijoita käytettiin kuljetuksiin, mutta myös Rooman laivastoa hyödynnettiin. Huomionarvoista oli senaatin tiukka ote armeijan toimista. Senaatin haluttiin hallitsevan armeijaa eikä päinvastoin, joten armeijan täytyi konsultoida senaattia hankkiakseen tarvikkeensa. Rooman merkittävä logistinen kykenevyys näkyi jokaisen armeijakunnan rakenteessa. Suuri erillinen yksikkö kehitettiin tukemaan logistiikan tarpeita, johon kuului esimerkiksi useita muuleja ohjaajineen, joskus jopa kuljetuskärryjä. Legioonaa kohden palveli noin 600–1200 muulia. Jos kuljetustarpeissa havaittiin puutteita, hyödynnettiin tällöin paikallisen omaisuuden haltuunottoa aina työhevosista miesvoimaan. Räikeänä esimerkkinä voidaan pitää paikallisen siviilin käskyttämistä kantamaan roomalaisen sotilaan varustusta tietyn matkaa. Roomalainen sotilas varustettiin sotaretkelle yhden viikon ruuat mukanaan, joita täydennettiin myöhemmin tuotavilla lisätoimituksilla. Täydennysruuat matkasivat joukkojen mukana niin sanotussa tavarajunassa. Sillä viitataan muuleilla tai muilla työeläimillä vedettäviin kärryihin, joiden valtavat kolonnat seurasivat rivisotilaiden marsseja. Aleksanteri Suuri (356–323 *eaa.*) kehitti tavarajunan konseptin huomatessaan sen helpottavan täydennyksien saamista etulinjaan. Roomalaisten valtaamien alueiden hallinta mahdollisti viljavarastojen rakentamisen tai haltuunoton, joka toistettuna johti useiden varastojen perustamiseen valtakunnan kaupunkien välille. Roomalaisten ylläpitämät valtakunnan halki ulottuvat huoltoyhteydet eivät ainoastaan taan-

neet onnistuneita aluevaltauksia, vaan ylläpitivät myös omia sotajoukkoja jo vallatuilla alueilla. Roomalaisten kuljetusyhteydet olivat edellä aikaansa ja kestikin vuosisatoja Rooman kaatumisen jälkeen ennen kuin siihen verrattavaa järjestelmää käytettiin uudelleen. (Williams 2020.)

Kaikkein merkittävimpänä pidettyä tietoa pronssikauden kaupankäynnistä ja sen logistiikasta Välimeren alueella saatiin kuuluisan kauppalaiva Uluburun hylystä, jonka uppoamisajankohdaksi on arvioitu 1300-lukua *eaa*. Hylyn uppoamispaikka on Turkin lounaisosassa sijaitsevan Kas'n kaupungin eteläpuolella noin 10 kilometriä rannasta. Reilu 15-metrinen laidoitettu vene lepää lähes 50 metrin syvyydessä. Vuosien 1984–1994 aikana muutaman kuukauden mittaisia sukelluskampanjoita järjestettiin löytöesineiden pelastamiseksi. Niiden aikana yksittäisiä sukelluksia toteutettiin yli 22 000 kappaletta. Pelastetuista esineistä muodostui yksi valtavimmista kokoelmista pronssiajan artefakteja, jotka ovat löydetty Välimeren alueelta. Laiva kuljetti muun muassa satoja kupariharkkoja, lasiharkkoja, tinaa, puutavaraa, keramiikkaa, kiviankkureita sekä arvokkaita mineraaleja. Mielenkiintoisen aluksen lastista tekee sen, että pronssitavaran paino ilman keramiikkaa on ollut 11 tonnin luokkaa. Kupariharkot olivat asetettu taitavasti aluksen etuosaan, joka mahdollisti hyvän painojakauman toteutumisen, kun harkkojen painoa tasapainotettiin muulla painavalla lastilla muun muassa ankkureilla, lasiharkoilla ja keramiikalla. Tämä käy esille kuviosta 1. (Stojić, Tanackov & Tepić 2011.)



Kuvio 1 Rekonstruktio kauppalaiva Uluburunin rahdin painojakaumasta laivan ruumassa (Stojić, Tanackov & Tepić 2011)

Näin ollen Uluburunin yhteenlaskettu paino saattoi olla jopa yli 20 tonnia. Monimutkaisen painojakauman takaaminen niin painavalle lastille edellyttää nykypäivänäkin merkittävän paljon tietotaitoa ja laskelmallisuutta, joten suoritusta voidaan pitää erityisen ammattitaitoisena ja koordinoituna. Navigoinnin lisääntyminen useiden eri kaupunkien satamiin mahdollisti erilaisen tavaran rahtaamisen laivoissa. Lisääntyneen tavaramäärän takia veneen miehistöt alkoivat pitämään kirjaa kaikista tavaroista, joita laiva kuljetti. Näin sai alkunsa merikuljetuksiin yhdistettävä tavarankuljettajan asiakirjaa eli konossementtia muistuttava asiapaperi. Sen tarkoituksena oli helpottaa tavaroiden käsittelyä laivoissa ja toimia vahvistuksena kuljetussopimuksesta, sekä tavaran vastaanotosta ja sen kuljetuksesta sovittuun määränpäähän (Merikuljetus n.d). Asiakirjan ylläpito vaati paljon suunnittelua niin käytettävien vesireittien kuin satamissa suoritettavien purkuoperaatioiden osalta, sillä aina rahtitavaroiden vaihtuessa laivan painojakauma ja tasapaino tuli määrittää uudestaan. Vesireittien alustava navigointi täytyi suorittaa ennen vesille lähtöä, joka itsessään mahdollisti sujuvan reaaliaikaisen navigoinnin Välimeren satamien välillä. Yllä mainitut toimenpiteet edellyttivät merkittävää kokonaisvaltaista käsitystä navigoinnista, sääolosuhteista, laivan teknisistä ominaisuuksista, riskianalyysistä, rahdattavista tuotteista,

rahdin järjestelystä ja kaupankäyntiasetuksista. Uluburun esimerkki täyttää käytännössä nykyaikaisen logistiikkajärjestelmän keskeiset piirteet. (Stojić, Tanackov & Tepić 2011.)

Alun perin logistiikan termiä on käytetty sveitsiläisen kenraalin Baron de Jominin (1779–1869) toimesta kun termi vieraannutettiin sotilasarvosta *Marechal de logis*, joka viittaa asevoimien tukijoukkojen organisointiin. Toinen logistiikkaan rinnastettava termi *loger* viittaa sotilasjoukkojen majoittamiseen kasarmeissa. Logistiikan käsite rantautui Yhdysvaltoihin 1900-luvulla, jolloin asevoimat ottivat sen välittömästi käyttöönsä kuvaamaan joukkojen kuljettamista ja varustamista. 1940-luvulla toisen maailmansodan aikaan termiä muokattiin vastaamaan suunnittelu- ja johtamisprosessia liittoutuneiden joukkojen uudelleen majoittamisessa ja huoltamisessa. Siviilialalla logistiikan käsite otettiin käyttöön vasta 1960-luvulla ja samalla sen merkitys muuttui sota-ajan kuljetuksista kuvaamaan fyysisten jakeluverkostojen suunnittelua ja toteuttamista. Professori Hans-Christian Pfohl uudisti logistiikkaa tieteenalana ja loi ominaiset tunnuspiirteet logistiikan kehittämiselle vuonna 1974. Nykyaika on mahdollistanut globaalin viestinnän, ajoneuvojen satelliittipaikannuksen, kehittyneet turvallisuusjärjestelmät sekä saumattoman yhteistyön eri organisaatioiden välille. Näistä riippumatta logistiikan periaate ja merkitys ovat pysyneet muuttumattomina. (Stojić, Tanackov & Tepić 2011.)

3.2 Logistiikka nykymuodossaan

”Logistiikan tavoite on saada oikea tuote oikeaan paikkaan mahdollisimman pienin kustannuksin halutulla palvelutasolla. Logistinen kokonaisuus käsittää̈ materiaali-, tieto- ja pääomavirrat ja ulottuu materiaalien hankintalähteiltä lopulliselle asiakkaalle asti.” (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

Nykyaikainen logistiikka kytkeytyy vahvasti talouteen ja se on toiminut myös yhtenä merkittävänä pilarina modernin talouden kehityksessä. Logistiikka omaa kehittyneen organisaatio- ja hallintorakenteen lisäksi tärkeän roolin yritysten ja kansantalouden kilpailukyvyn parantamisessa, teollisen infrastruktuurin tehostamisessa, sekä infor-

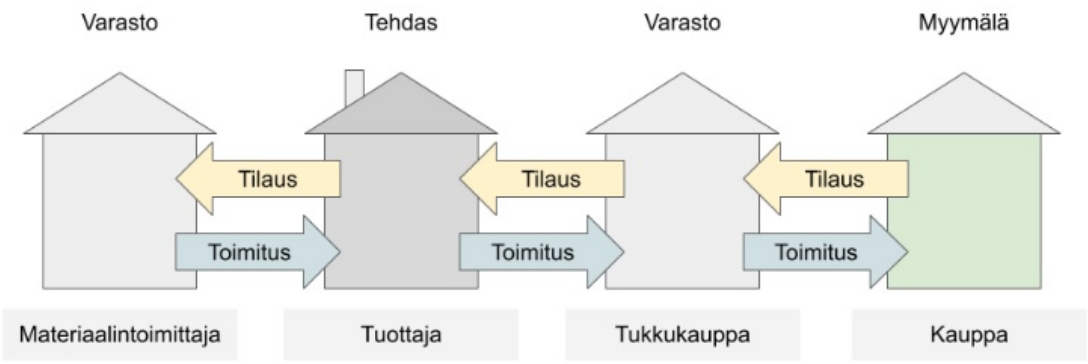
maatioteknologian edistämisessä. Liikeyritykset, valtiot ja tutkimuslaitokset arvostavat logistiikkaa alana, jonka tiedetään kehittyneen ja edelleen kehittyvän nopeasti. Vaikka moderni logistiikka on vaatinut rakentuakseen suuren määrän pääomaa, tarvikkeita ja hallinnointia, niitä ei voida pitää yksinomaan vastuussa sen muodostumisesta ja kehittymisestä nykyiseen muotoonsa. Tuntemamme logistiikan muotoutumisessa on paljon yhtäläisyyksiä kehittyneen yritysjohtamisjärjestelmän kanssa ja logistiikkateollisuuden tekninen perusta onkin hyötynyt merkittävästi viestintätekniikan ja johtamisen kehittymisestä. Kuljetusteollisuus nähdään alati kehittyvänä, pieniä parannuksia säännöllisesti tekevänä tahona, mutta todellisuus eriää tästä tulkinnasta. Uudenlainen logistiikan uudistus muodostuu aina kun yhteiskunta kehittää itseään niin, että hyödykkeiden kuljetus ja hallinnointitavat uudistuvat. (Dong 2013.)

Logistiikan toiminnot jakautuvat karkeasti varastointiin, rahdin käsittelyyn, kuljetukseen, toimitusketjun hallintaan ja toiminnanohjaukseen. Prosessit eivät ole aina näyttäneet tältä, vaan ne ovat kehittyneet historian aikakausien mukaan kulutusyhteiskunnan mukana. Logistiikkateollisuuden kehitys on käynyt läpi kolme vaihetta historiansa aikana: perinteinen tuotantologistiikka, kuljetus- ja varastointilogistiikka, sekä moderni logistiikka. Perinteiset kuljetus- ja varastointilogistiikan palvelut sisältävät yleensä kuljetuksen, varastoinnin, lastaamisen ja purkamisen. Palvelut koostuvat kahdentyyppisistä organisaatioista, laajoista varastointi- ja kuljetusyrityksistä, sekä itse varastointi- ja kuljetusosastoista, jotka toimivat myyjien ja tukkukauppiaiden sisällä. Kuljetus- ja varastointilogistiikan palvelut ovat keino saada tuotteet kuluttajille, jolloin kuljetettavat tuotteet varastoitiin tuottajien varastohalleihin. Myöhemmin suurimmat toimijat alalla perustivat omia logistiikkakeskuksiaan tehostamaan kasvavaa toimintaa, mutta yleisesti liiketoiminnalliset kontaktit logistiikkayrityksissä olivat vähäiset ja ainoa yhteys yritysten ja valmistajien välillä oli materiaalien siirtäminen. Tavanomainen varastointilogistiikka on suosittu toimintatapa edelleen, mutta yritykset ovat hakeutuneet entistä suuremmalla kiinnostuksella tuottavampien kuljetustoimien pariin. Moderni logistiikka seuraa perinteisen kuljetus- ja varastointilogistiikan jalanjälkiä, mutta eroaa vahvasti toimintatavoissaan muun muassa tuomalla kuvioon mukaan erilaisia alihankkijoita ajatuksena tehostaa toimintaansa. Kiihtyvän globaalin talouden kasvu yhdistettynä tuotteiden elinkaaren lyhenemiseen ja kilpailukyvyn

jyrkkään nousuun yritysten välillä on merkityksellään aiheuttanut modernin logistiikan mukautumisen tämän aikakauden vaatimuksiin. Kuljetusalan mukautuminen nykymaailman haasteisiin on luonut monia toimintoja, joista ovat hyötyneet monet toimijat eri alojen parissa. Logistiikan globaali toiminta useiden eri alojen yritysten kanssa on vaikuttanut positiivisesti yhteistyön rakentumiseen organisaatioiden välille. Kun perinteinen logistiikka keskittyi enemmän yhteistyöhön varastojen välillä, pyrkii moderni logistiikka korostamaan yhteistyötä koko hankintaketjujen osapuolten välillä ja täten yhdistämään kuljetusalan toimintoja muiden alojen kanssa. Logistiikan korkeat vaatimukset ajankäytön hallintaa ja palveluiden automatisointia, sekä sujuvoittamista koskien ovat voimavaroja, joihin jokaisen yrityksen tulee panostaa maksimoidakseen yritystoimintansa. Nykyaikainen logistiikka toimii järjestelmällisesti sulauttaen yhteen monet toiminnot, jotka eivät ole aikaisemmin olleet osa kuljetuskokonaisuutta. Tämä mahdollistaa koordinoidun toiminnan kolmannen osapuolten tilojen ja tekniikan kesken edesauttaen tavaroiden toimittamista nopeasti ja turvallisesti matalilla kustannuksilla. Nykyään kuljetusyritykset hallitsevat valtavia rahtilaivastojaan edistyneen tietoverkkotekniikan välityksellä ja pystyvät valvomaan valtavia määriä rahtia, sen jokaisessa käsittelyvaiheessa varmistaen niiden pääsyn päämääräänsä. (Dong 2013.)

3.3 Logistiikan toimitusketjun osa-alueet

Logistiikan toimitusketju muodostuu monesta toimijaorganisaatiosta, jotka yhdessä pyrkivät ohjamaan materiaali- tai palvelukokonaisuuksia ja kehittämään niitä, jotta ketjusta saadaan mahdollisimman tuottava ja toimiva järjestelmä. Yksinkertainen tilaus-toimitusketjun toiminta-ajatus näkyy kuviossa 2. Nimensä mukaisesti ketju toimii tilausperiaatteella, jossa kuluttajalle hyödykkeen toimittava tai myyvä kauppa tilaa hyödykkeensä tukkukaupalta, joka tilaa hyödykkeensä tuottajalta, joka tilaa materiaalinsa materiaalintoimittajalta. Valmistuvan hyödykkeen toimitus asiakkaalle tapahtuu päinvastaisessa järjestyksessä tilaukseen nähden. (Logistiikka ja toimitusketju n.d.)



Kuvio 2 Tilaus-toimitusketju (Logistiikka ja toimitusketju n.d.)

Riippumatta liiketoimialueesta (Supply Chain Management) toimintaketjut sisältävät lukuisia organisaatioita, jolloin niiden hallinta on tärkeää kokonaisuuden ylläpitämiseksi. Supply Chain Managementilla kuvataan palveluiden ja hyödykkeiden hallinnointia sisällyttäen kaikki toiminnot materiaalien valmistuksesta lopputuotteen toimittamiseen asiakkaalle. Toimitusketjun hallinnassa painotetaan ketjun osapuolten yhteistyön sujuvuutta koko toimitusketjun toiminnan optimoimiseksi. (Logistiikka ja toimitusketju n.d.)

Yhteiskuntaan kielteisesti vaikuttaneet tapahtumat ovat osaltaan säännelleet negatiivisesti toimitusketjujen huoltovarmuutta viime vuosien aikana. Koronavirus, Brexit, Japanin maanjäristykset ja monet muut ilmiöt ovat heikentäneet logistiikan toimivuutta ja kuormittaneet kuljetuspalveluita ympäri maailmaa. Olemme suomalaisina saaneet itsekin kokea toimitusketjujen heikentyneen toimivuuden koronaviruksen takia. Raaka-aineiden ja komponenttien hankinnan ja tuotteiden toimituksen hidastuminen sekä muut alaa rasittavat tekijät kuten polttoaineiden hinnan nousu sekä työpaikkoihin ja palkan korotuksiin liittyvät epävarmuudet ovat ajaneet yritykset miettimään toimitusketjujen kehittämistä yhä joustavimmiksi, jotta tulevaisuuden vaativat tapahtumat eivät kuormittaisi ketjuja yhtä paljon kuin aikaisemmin. Toimitusketjujen tulee olla joustavasti suunniteltuja, sillä niihin vaikuttavia kuljetusaikataulujen venymisiä ja niiden muokkauksia tapahtuu päivittäin, joihin yrityksien täytyy mukautua. Joustavuutta on mahdollista parantaa erilaisin keinoin esimerkiksi teknisillä paran-

nuksilla, joita ovat muun muassa varastopinta-alan laajentaminen ja kapasiteetin kasvattaminen. Tuotanto- ja hankintaverkoston kasvattaminen, sekä hyödykkeiden kokoonpanon tai alihankkijoiden tuominen lähemmäs asiakkaita kasvattavat myös toimitusketjun joustavuutta. (Haverinen 2020.)

3.4 Logistiikan kuljetusmuodot

Kuljetusmuodon valintaan vaikuttaa saatavilla olevat kuljetusvaihtoehdot. Niitä harkitessa on tarkasteltava kustannuksia, käytettäviä reittejä ja niiden pituuksia sekä kuljetukseen kuluvaa aikaa. On hyvä puntaroida myös kuljetettavan tavaran teknisiä ominaisuuksia kuten arvoa, pakkausmuotoa, lastausta ja purkua sekä mahdollisia riskitekijöitä, jotka vaikuttavat kuljetukseen. Kuljetusmuotoja ovat esimerkiksi lentokuljetukset, maantiekuljetukset, rautatiekuljetukset, yhteiskuljetukset, sekä vesikuljetukset, jotka jakautuvat sisävesi- ja merikuljetuksiin. (Kuljetukset n.d.)

Lentokuljetukset

Lentokuljetukset ovat kallis kuljetusmuoto johtuen koneiden valtavista lentotuntikustannuksista. Rahtimäärät ovat pienempiä kuin muilla kuljetusmuodoilla rajallisen tilan takia, joka rajaa kuljetettavat tuotteet koon ja painon takia pieniksi. Nopea ja luotettava kuljetusmuoto sopii esimerkiksi kallisarvoiselle ja kiireelliselle rahdille. (Tapaninen n.d.)

Maantiekuljetukset

1970-luvun aikana maantiekuljetukset alkoivat muuttua yhä käytetymmäksi vaihtoehdoksi vastaamaan kuljetusalan tarpeeseen mukautuvalle ja nopealle kuljetusmuodolle. Suomen lisäksi maailmanlaajuisesti muissa teollisuusmaissa maantiekuljetukset toimivat tärkeimpänä muotona tavaroiden sisäiselle rahtaamiselle, mutta myös suuri osa maanosien sisällä tapahtuvista kansainvälisistä vientikuljetuksista liikkuvat maanteitä pitkin. Tiekuljetukset sopivat paremmin kuin hyvin lyhyen matkan jakelukuljetuksiin sekä kuljetushubien eli terminaalien välisiin siirtoihin. (Tapaninen n.d.)

Rautatiekuljetukset

Raskaat ja säännölliset kuljetukset käyttävät pääsääntöisesti rautateitä tavaran siirtoon. Kotimaiset metsä- ja metalliteollisuuden vientituotteet kuten paperi, kartonki sekä erilaiset raaka-ainekuljetukset hyötyvät Suomen rautatieverkostosta samoin kuin valtakuntamme läpi kulkeva Venäjältä tuleva kauttakulkuliikenne. (Tapaninen n.d.)

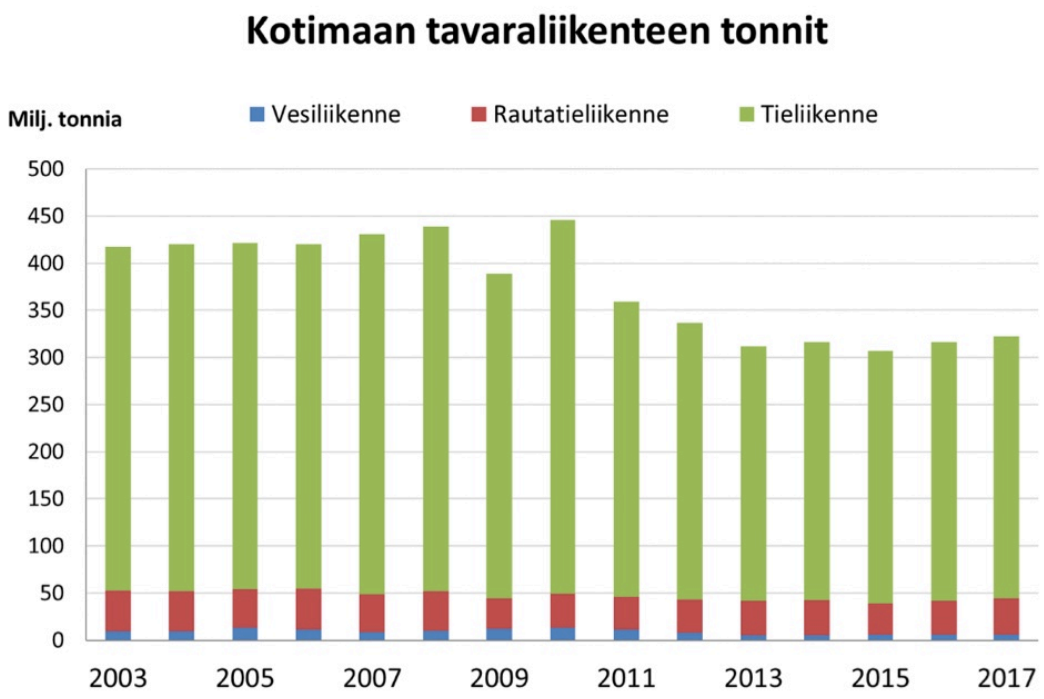
Vesikuljetukset

Veden ylitse tapahtuvilla sisävesi- ja merikuljetuksilla kuljetetaan enemmän rahtia kuin millään muulla kuljetusmuodolla. Lyömättömän kilpailukyvyn tarjoama tilakapasiteetti mahdollistaa raskaiden tai suurien tavaroiden rahdin. Esimerkiksi teolliset raaka-aineet, joiden kuljetus ei ole kannattavaa muilla kuljetusmuodoilla käyttävät vesikuljetuksia. (Tapaninen n.d.)

Yhteiskuljetukset

Yhteiskuljetukset toimivat kahden tai useamman kuljetusmuodon kokonaisuutena. Ne lento-, meri- tai rautatiekuljetukset, joiden päämäärä on muualla kuin satama- ja terminaalialueella edellyttävät maantiekuljetuksen käyttöä tavaran kuljetukseen päämääräänsä. Esimerkiksi metsäteollisuuden raaka-aineet kulkevat säännöllisesti rautateiden ja maanteiden yhteiskuljetuksilla. (Tapaninen n.d.)

Kotimaanliikenteessä käytetyin kuljetusmuoto on maantiekuljetus johtuen laajasta ja kattavasta tieverkostosta kun taas Suomen ulkomaankaupassa suositaan vesiteitse käytettävää kuljetusta. Kotimaan rahtimäärät pois lukien lentokuljetukset vuosien 2003–2017 aikana ovat eritelty kuviossa 3. (Tapaninen n.d.)



Kuvio 3 Kotimaan tavaraliikenteen volyymi (Tapaninen n.d.)

4 Logistiikan tietojärjestelmät

Yritysten ja julkisen sektorin logistiikan parissa eletään muutoksen aikaa. Digitalisaatio ja tekoäly ovat vaikuttamassa alan kehittymiseen ja toimivat tärkeinä ponnahduslautoina kohti toimintojen yhtenäistämistä. Kuljetusyritykset hyötyvät digitalisaation tuomasta lisäarvosta niin tuotannon tehostamisessa kuin kustannuksien alentamisessakin. Tulevaisuus näyttää tekoälyn yleistymisen vaikutuksen yksityisten- ja julkisen sektorin kuljetusyrityksien toimintoihin, mutta alustavat näkemykset vaikuttavat alaa mullistavilta (Digitaalisuus logistiikassa n.d). Digitalisaation merkitys on kasvanut kuljetus- ja logistiikan liiketoiminnassa kansainvälisten verkkokauppojen muuttaessa toimintaansa yhä enemmän logistiikkaoperaattoreiden suuntaiseksi. Satamat ja varustamot luovat valtavia digitaalisia alustoja vesikuljetusten integroimiseksi muihin kuljetusmuotoihin ja toimijoihin. Tämä toimii hyvänä esimerkkinä kuljetusmuotojen yhtenäistämisestä ja kehittämisestä jokaisen kuljetussektorin tarpeisiin sopivaksi. (Dahlberg, Korpela, Lammi, Lankinen, Mikkonen, Nykänen 2019.)

Liikenne- ja viestintäministeriön toteuttamassa Hajaantuneesta hajautettuun -hankkeessa logistiikan digitalisaatiostrategian valmistelemiseksi (2019) pyrittiin tuomaan esille keinoja digitalisaatiokehityksen vahvistamiseksi logistiikka-alalla. Kiihdyttämällä digitalisaatiokehitystä logistiikkasektorilla pyritään kustannustehokkuuteen ja päästövähennyksiin. Manuaalisesta tietojen käsittelystä pyritään siirtymään täysin digitaalisiin tiedonsiirtomenetelmiin niiden toimijoiden keskuudessa, jotka vielä toimivat fyysisiä menetelmiä käyttäen. Tämä vaatii merkittäviä uudistuksia logistiikan toimintoihin ja teknologioihin. Muun muassa sähköisen tiedonsiirtoon ja allekirjoituksiin päivittäminen edellyttää ohjauksen ja pilottihankkeiden kokeilua, jotta muutoksen nähdään olevan myönteisesti yrityksien toimintoihin vaikuttava parannustoimenpide. (Dahlberg, Korpela, Lammi, Lankinen, Mikkonen, Nykänen 2019.)

Logistiikassa käytettävä tietoverkosto koostuu kolmesta osasta: tunnistusjärjestelmästä, materiaalinohjauksesta ja niitä hallitsevasta tietoverkkojärjestelmästä. Tunnistusjärjestelmä sisältää organisaatioiden välisen tiedonsiirron (EDI, Electronic Data Interchange) ja automaattisen laiteen tunnistustekniikan (AEI, Automatic equipment identification). Organisaatioiden välinen tiedonsiirto tarkoittaa yksinkertaisuudessaan tietojen siirtoa tietojärjestelmästä toiseen yrityksen tietojärjestelmään. Tiedonsiirto toimii sovittujen standardien mukaisesti, joiden perusteella jaettava informaatio määräytyy. Siirryttäessä paperisten dokumenttien täyttämisestä täysin sähköisesti hallittaviin tietojärjestelmäkokonaisuuksiin, jossa eri organisaatiot keskustelevat keskenään saumattomasti, parannetaan logistiikan hallittavuutta verrattuna perinteiseen toimintaan. (Dong 2013.)

Tieliikenteessä tapahtuvien kuljetuksien ajoneuvokohtainen tietojärjestelmä käsittää esimerkiksi taulutietokoneen eli tabletin, GSM-datayhteyden (Global System for Mobile communication) ja viivakoodinlukijan. Tabletilla rahtaaja hallinnoi ja käsittelee tietoja kuljetuksestaan viivakoodinlukijan rekisteröidessä tietoja vaihtuvasta rahdista, kun taas GSM-datayhteys mahdollistaa tiedonsiirron ajoneuvon rahtikirjan ja logistiikkayrityksen tietojärjestelmien välillä. Yhä useammissa kuljetusyrityksien ajoneuvoissa alkaa näkyä GPS-paikannustekniikkaa (Global Positioning System), jolloin yritys pysyy selvillä kuljetuksiensa tilasta. Paikannustekniikka mahdollistaa myös informaa-

tion jakamisen asiakkaalle, joka voi seurata pakettiaan Internetin kautta tiettyjen tilannetietojen perusteella. Palvelu on usein maksuton asiakkaalle, joskin kuljetusyritykselle koituvat taloudelliset menot on sisällytetty rahtipalvelun hintaan. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

Lentoliikenteessä rahtiyhtiöiden toimintaa määrittää pitkälti Kansainvälisen ilmakuljetusliiton (IATA, International Air Transport Association) standardit siitä miten kuljetuksia hallinnoidaan. Rahtiyhtiöt saattavat tarjota myös omia seurantajärjestelmiään asiakkaidensa käyttöön esimerkiksi rahtikirjan numeron perusteella tapahtuvaa seurantaa varten, kuten esimerkiksi Finnair Cargo. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

Rahtilaivaliikenteen helpottamiseksi, Intermodal Portal- niminen järjestelmä on kehitetty Euroopassa operoivien satamien tietojärjestelmien rinnalle ohjaamaan tietoliikennettä satamien ja niiden kanssa operoivien toimijoiden välillä internetpohjaisella käyttöliittymällä tai käyttäen XML-sanomia (Extensible Markup Language) tiedonsiirtoon. Tavoite on jakaa tietoa rahtialuksen matkareitistä ja lastista seuraavaan kohdesatamaan. Suomessa nykyisin toimiva Port@Net -järjestelmä siirtyy hiljalleen Intermodal Portal -järjestelmäksi, joka mahdollistaa toimiessaan sujuvan tiedonsiirron Itämeren ja Pohjanmeren satamien välillä. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

Erilaisia seurantajärjestelmiä hyödynnetään myös rautatieliikenteessä käyttäen esimerkiksi RailTrace-järjestelmää, joka on eurooppalaisten rautatie- ja logistiikkayhtiöiden yhteistyössä kehittämä palvelu. Tämä kansainvälinen vaunujen sekä lähetysten seurantaan perustuva järjestelmä on käytössä melkein koko Eurooppaa myöten. Myös Suomen VR Cargo sekä Venäjä mahdollistavat rahdin jäljittämisen yhdistämällä lähetys- ja vaunutiedot keskenään yhdeksi tiedostoksi. Internetin välityksellä toimiva RailTrace toimii ajantasaisesti yhdistäen eri yhtiöiltä saamansa tiedot yhdeksi kokonaisuudeksi, joka optimoi kuljetuksien valvonnan sekä raportoi mahdollisista häiriötilanteista kuten myöhästymisistä. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

Edellä mainittujen liikennekuljetuspalveluiden lisäksi on olemassa niin sanottujen pikarahtiyhtiöiden tai pikakuriirien tarjoamat maksulliset rahtipalvelut. Normaalia nopeampi kuljetus on tarkoitettu rahdille, joka vaatii syystä tai toisesta mahdollisimman nopean kuljetuksen määränpäähänsä. Lisäpalvelu on maksullinen ja normaalisti hieman kalliimpi vaihtoehto mutta tarjoaa asiakkaalle lähetyksen seurannan, joka yleensä kattaa koko maapallon ja tarjoaa vapauden tarkistaa lähetyksen tilan ja sijainnin hetkenä minä hyvänsä. Pikalähetyksiä skannataan useassa matkan vaiheessa ja tieto välitetään asiakkaalle järjestelmään, josta tilan voi tarkistaa esimerkiksi rahtiyhtiön asiakaspalvelun, sähköpostin tai matkapuhelimen kautta. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

4.1 Paikannus- ja seurantateknologiat

Talouden ja kulutuksen kasvaessa myös logistiikka-ala laajentuu kasvavan kysynnän myötä. Toimitusketjut muuttuvat toimitusverkostoiksi, joiden vaatimusten mukaisesti rajautuvat halutut kuljetusmuodot ja toimijat. Kuljetusten aikatauluttaminen nousee yhä korkeampaan asemaan ja tiedon tarve kuljetusketjun jokaisessa osassa kasvaa entisestään. Asiakkaiden vaatimukset toimivalle kuljetusketjulle pitävät sisällään rahdin sijainnin ja sen kuljetuksen tilan reaaliaikaisen jakamisen asiakkaalle. Kuljetuksen tilannetieto siitä onko tavara esimerkiksi kuljetuksessa, varastolla vai luovutettu asiakkaalle on tärkeää ensisijaisesti kuljetusyrityksen tuotannonohjaukselle, jotta tavaravirtojen sujuvuus saadaan maksimoitua. Tiettyjen kuljetustarvikkeiden seuranta on tarpeellista ja osa suurista kuljetusyrityksistä ja heidän asiakasyrityksistään ovat rakentaneet koko kuljetusketjun kattavia alajärjestelmiä, jotka ovat räätälöity yritysten omiin vaatimuksiin kuljetuksien seurantaa varten. Suuret kuljetusyritykset vastaavat lukemattomista määristä kuljetuksia, jotka vaativat jatkuvaa seurantaa kuljetusketjun jokaisessa vaiheessa. Talouden kasvun ja kansainvälistymisen johdosta edellytetään yhä useampien kulkumuotojen ja organisaatioiden yhteistyötä kuljetusten onnistumiseksi. Tämän takia standardoitu yhtenäinen seurantajärjestelmä on edellytys yhteiselle toiminnalle. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

Yritykset kokevat hyötyvän seurantajärjestelmistä, sillä niiden avulla he pystyvät hallitsemaan tehokkaammin logistisia prosessejaan. Tiedonsiirtojärjestelmät, reitin optimointijärjestelmät ja langattomat paikannus- ja seurantajärjestelmät toimivat parantaen logistiikkatoimintojen läpinäkyvyyttä ja toiminnanohjausmahdollisuuksia. Yrityksen on oleellista tutkia kuinka seurantajärjestelmän hankkiminen parantaisi kuljetuspalveluita ja onko se taloudellisesti kannattava investointi pidemmällä aikavälillä. Yleensä seurantajärjestelmä tuottaa parempaa palvelua käyttäjäyritykselleen ja lisäarvoa asiakkailleen. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

Satelliittipaikannus

Avaruudessa maapalloa kiertävät satelliitit mahdollistavat tarkan paikkatiedon radioaaltoja hyödyntämällä. Satelliitti lähettää radioaaltoja vastaanottajalaitteelle ja sijainti lasketaan useamman eri satelliitin lähettämän signaalin kulkuajoista. Näköyhteys on välttämätön paikannuksen toiminnan kannalta. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.) Logistiikka- ja kuljetusyritykset käyttävät satelliittipaikannusjärjestelmiä muun muassa kuljetusvälineiden sijaintitietojen hyödyntämiseen liiketoiminnan tehostamisessa. GNSS-satelliittipaikannusjärjestelmiä (Global Navigation System) käytetään paikannuksen lisäksi myös tarkan aikatiedon hyödyntämiseen erilaisten tietojärjestelmien synkronoinnissa. Satelliittipaikannuksen käyttäjät vaihtelevat juoksulenkkinsä pituuden mittaavasta yksityishenkilöstä logistiikka-alan moniyrityksiin ja julkisen palvelun turvajärjestelmien käyttäjiin. GNSS-paikannusjärjestelmiin kuuluu neljä maailmanlaajuisesti toimivaa paikannusjärjestelmää: Galileo, GPS, GLONASS ja BeiDou. Paikannusjärjestelmät eroavat teknisiltä ominaisuuksiltaan, mutta perusperiaate on kaikilla sama: tuottaa luotettavaa maailmanlaajuista sijainti- ja aikatietoa. Euroopan unionin omistama siviiliviranomaisten hallinnoima paikannusjärjestelmä Galileo on rakennettu toimimaan omavaraisena satelliittipaikannusjärjestelmänä, joka mahdollistaa kriittisen teknologian toiminnan sitoutumatta Euroopan ulkopuolisen toimijan paikannusjärjestelmään. (Vihavainen 2020.) Global Positioning System on Yhdysvaltain puolustushallinnon kehittämä maailman käytetyin paikannusjärjestelmä. Sen satelliittipaikannuksen peruspalvelut otettiin

käyttöön 1990-luvun puolessa välissä, mutta GPS-projektia (entinen NavStar) aloitettiin kehittämään jo 1970-luvulla tarkoituksenaan tuottaa paikka- ja aikatietoa sotilaskäyttöön. Neuvostoliiton alas ampuma Korean Airin lento 007 aikaansai silloisen Yhdysvaltain presidentin Ronald Reaganin hyväksymään GPS-järjestelmän siviilikäyttöön, jotta vastaavilta navigointivirheiden aiheuttamilta tragedioilta vältyttäisiin. (Frelinger, Frost, Fossum, Lachow, Pace, Pinto & Wassem 1995.) Taulukossa 1 ilmenee yksityiskohtaista tietoa edellä mainittujen paikannusjärjestelmistä.

Taulukko 1 GNSS-palveluiden tekniset ominaisuudet (Vihavainen 2020)

	Galileo	GPS	GLONASS	BeiDou
Hallinnoija	EU	USA	Venäjä	Kiina
Peruspalveluiden käyttöönotto	Käytössä vuodesta 2016	Käytössä vuodesta 1995	Käytössä vuodesta 1993	Käyttöönotto 2020
Satelliittien lukumäärä	24+6	31+1	23+4	30
Sijaintitiedon tarkkuus	• Peruspalvelu 1-2 m • Tarkkuuspalvelu (HAS) 0,2 m	2-5 m	10 m	10 m
Aikapalvelun tarkkuus	< 15 ns	< 20 ns	-	< 20 ns

Galileo ja GPS tarjoavat huomattavasti täsmällisemmän sijaintitiedon tarkkuuden verrattuna itäisten suurvaltojen GNSS-järjestelmiin. Galileo mahdollistaa sijaintitiedon jopa 20 cm tarkkuudella käyttämällä HAS-palvelua (High Accuracy Service), jolloin herää kysymys nykyisten järjestelmien kehittämisen tarpeellisuudesta entistä tehokkaimmiksi. Yksityiskäyttäjä suoriutuu karttapalveluiden käytöstä nykyisten järjestelmien tarkkuuksilla, mutta yritykset ja valtiolliset toimijat erityisesti puolustus- ja turvallisuusalalla vaativat yhä tarkempia ja luotettavia sijaintitietojärjestelmiä eri käyttötarkoituksiin. Tämän takia Galileon järjestelmä kehitettiin mukautumaan viranomaiskäyttöön muun muassa tuomalla saataville täysin viranomaiskäyttöön räätälöity PRS-palvelu (Public Regulated Service). Se tarjoaa jatkuvaa sijainti- ja aikatietoa viranomaistoiminnan lisäksi myös elintärkeälle infrastruktuurille. Kyseisiä palveluita ovat esimerkiksi infrastruktuurin ylläpitoon tarkoitetut järjestelmät kuten telekommunikaatioverkot ja sähkön siirto- ja jakeluverot. Galileonin erityispalvelut antavat

myös tuen maailmanlaajuiselle Cospas-Sarsat-hätäsignaalijärjestelmälle, joka mahdollistaa etsintä- ja pelastuspalveluiden käytön omalla radiolähettimellä. (Vihavainen 2020.) Cospas-Sarsat on otettu käyttöön 1982. Suunniteltu hyödyntäen satelliitteja ja signaalinvastaanottajakeskuksia maan pinnalla, järjestelmä tuottaa hätäsignaali- ja paikkatietoja etsintä- ja pelastuspalveluiden käyttöön riippumatta hädässä olevan sijainnista. Järjestelmän tehokkuutta kuvaa vuonna 2016 pelastettujen ihmisten määrä: 2000 ihmistä pelastettiin käyttäen Cospas-Sarsat -järjestelmää. Hätäsignaalijärjestelmä kehitettiin hiljattain uudeksi MEOSAR-järjestelmäksi (Medium Earth Orbiting Search and Rescue), joka toi välittömän ja maailmanlaajuisen paikannuskyvyn osaksi järjestelmää. (Delcuvellerie 2018.) MEOSAR-satelliittien etsintä- ja pelastuslähettimien avulla järjestelmä mahdollistaa vakaan ja vikasietoisen satelliittiviestintäyhteyden hätäsignaalilähettimen ja satelliitin välille sekä päivityskyvyn tuleville SAR-päivityksille. (Galileo’s contribution to the MEOSAR system. n.d.)

4.2 Tunnistustekniikat

Laajalti käytettyjä tunnistustekniikoita ovat RFID (Radio Frequency Identification), viivakooditunnistaminen ja optinen tekstintunnistus. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

RFID on etätunnisteilla toimiva tekniikka tiedon etälukuun ja tallentamiseen radiotaajuuksia käyttäen. Se on yksi maailman käytetyin seuranta- ja rekisteröintitekniikka, joka on hiljalleen korvaamassa perinteisen viivakooditunnistamisen. RFID:n komponentit toimivat lähettäen ja vastaanottaen viestejä. Komponentteihin lukeutuvat lukulaite, antenni, saattomuisti eli tunniste ja prosessori, joka käsittelee vastaanotetut viestit ja tallentaa ne tulevia lähetyksiä varten. Tunnistustekniikkana RFID on erittäin hyödyllinen sen monipuolisten ominaisuuksien takia:

- Radiotaajuuksien säätö vaikuttaa positiivisesti laitteen lukuominaisuuksiin
- Tunnisteen asento voi olla eriävä lukulaitteen asennosta.
- Tunnistus on mahdollista toteuttaa täysin automatisoidusti
- Näköyhteys ei ole vaatimus tunnisteen lukemiselle
- Useampia tunnisteita on mahdollista lukea samanaikaisesti

- Tunnisteiden yksityiskohtaisia tietoja voidaan muokata kuljetuksen aikana
- Luettavan tunnisteen etäisyys lukulaitteesta voi olla jopa 100 metriä (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

Käyttötarkoituksia RFID-teknologialle ovat esimerkiksi kulunvalvonta, tuotannonohjaus ja rahdin käsittely. Sen avulla parannetaan kuljetuksien luotettavuutta, ajanhallintaa sekä säästetään käsittelykuluissa. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

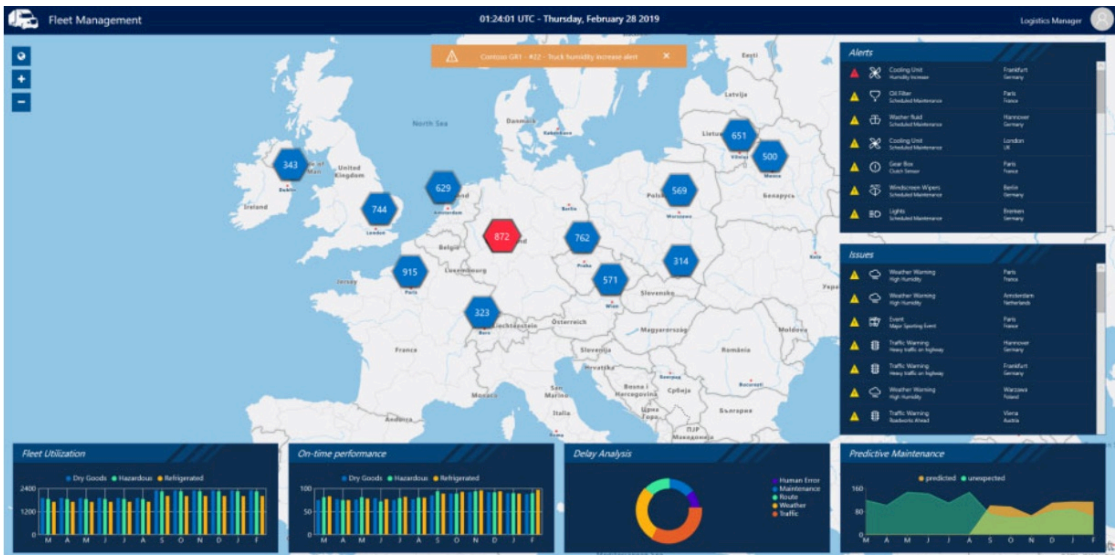
Viivakoodi on maailmanlaajuisesti käytetty tunnistustekniikka, jonka suosio selittyy sen monipuolisuudella ja yksinkertaisuudella. Sitä voidaan käyttää paperisena tarrana tai merkittynä suoraan tuotteeseen etsausmenetelmää käyttäen. Tällä hetkellä viivakoodin luku vaatii näköyhteyden koodin ja lukulaitteen välillä mutta kehitteillä on tekniikka, joka mahdollistaisi koodin luvun monen eri materiaalikerroksen läpi. Yleisiä viivakoodimerkintätapoja ovat lineaariset viivakoodit, joita ovat muun muassa kauppojen tuotteissa käytettävät EAN-koodit (International Article Number). Kaksiulotteiset viivakoodit lisäävät lineaariseen koodiin vertikaaliset viivat, jolloin koodien merkkimäärä tuplaantuu. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

Tekstin tunnistamien esimerkiksi rahtiliikenteen rekisterikilvistä tai kuljetuskonteista tapahtuu optisella tekstintunnistuksella – OCR:llä (Optical Character Recognition). Huomionarvoista on tekniikan kallis hankintahinta, jonka takia sen käyttö on vähäistä. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

4.3 Seurantapalvelu - Microsoft Azure IoT

Toimitusketjun luotettavuus perustuu tietoon lähetyksen tilasta ja tarkasta sijainnista kuljetuksen kaikissa vaiheissa. Perinteisesti toimitusketjujen toimijat seuraavat lähetyksiään paikkatiedon perusteella, joka saadaan niin sanotuista kriittistä matkapisteistä kuten satamista sekä aina kuljetusta operoivan toimijan vaihtuessa. Nykyaikana on syntynyt tarve lähetyksen jatkuvasta tila- ja sijaintitiedon reaaliaikaiseen

tarkkailuun, varsinkin kuljetettaessa arvokkaampia lähetyksiä kuten esimerkiksi tietotekniikkaa. Tuotteiden kokonaisvaltainen seuraaminen minimoi menetys- ja viivästysriskejä niiden kuljetuksessa. Tämän perusteella Microsoft ja sen kumppanin C.H. Robinsonin Technology Solutions for Logistics, Supply Chain and Freight Management / TMS ovat ottaneet käyttöönsä Microsoftin rakentaman Azure IoT Central -palvelun varmistuakseen tuotteiden valvonnasta kuljetuksien aikana. Microsoft hyödyntää Azure IoT Central -palveluaan esimerkiksi Xbox-pelikonsoleidensa ja Surface-tietokoneidensa kuljetuksissa. (Microsoft logistics team gains supply chain visibility using Azure IoT Central 2020.) Azure on Microsoftin 2008 julkaisema pilvipalvelujärjestelmä, joka pitää sisällään muun muassa edellä mainitun Azure IoT Central- palvelun. Azure IoT Central- palvelu on IoT-laitteiden hallintaan kehitetty kokonaisuus, joka sisältää erilaisia palvelukokonaisuuksia ja keskittyy vähentämään IoT-laitteiden kehittämisen, hallinnan ja ylläpidon rasitetta ja pääomamenoja sekä tuottamaan helposti hallittavaa ja monitoroitua informaatiota verkkoon yhdistettävistä Internet Of Things- laitteista. Azure IoT Central- palvelu mahdollistaa tehokkaan ja luotettavan kuljetusinfrastruktuurin, tieolosuhteiden arvion sekä reaaliaikaisen liikennetilanteen. Microsoftin Azure Maps- palvelun tarjoamat reaaliaikaiset laite- ja sijaintitiedot auttavat kuljetusreittien optimoinnissa, seurannassa, sekä kuljetustehokkuuden tarkkailussa. Kuviossa 4 näkyy Azure IoT Central- palvelun karttanäkymä ja kuljetuskaluston sijaintitiedot. Kuvio 5 esittää tilannekuvan kuljetuskaluston huomiota vaativasta jäähdytysjärjestelmän hälytyksestä, sekä reitinohjauksen lähimmälle varastolle kuorman tilan vakauttamista varten. Järjestelmä ottaa huomioon kuljetuksen erityistarpeet esimerkiksi vaarallisen aineen kuljetuksen ja huomioi tämän kuljetuksen reitittämisessä varastolle. (IoT in transportation and logistics n.d.)



Kuvio 4 Azure IoT- palvelun karttapalvelu (IoT in transportation and logistics n.d.)

Azure IoT Central- palvelu toimii yhdistämällä Internet of Things- laitteiden laitekohtaiset tiedot pilvipalveluun ja rakentamalla niistä käyttäjäystävällisen käyttöliittymän asiakkaalle laitteiden seuraamiseen. Microsoft myy käyttöpalveluaan yrityksille, mutta seurantalaitteiden hankkimisesta ja päivittämisestä vastaa asiakasyritys itse. (What is Azure IoT Central? n.d.)

Varmistaakseen datansiirron ja kommunikaatioviestit seurantalaitteiden ja pilvipalvelun välillä Microsoft on kehittänyt Azure IoT Hub- palvelun, joka toimii IoT Central-hallintajärjestelmän sisällä. Hub mahdollistaa turvallisen datansiirron molemminpuolisesti hallinnoiden jokaisen seurantalaitteen yksityiskohtaisia järjestelmäkoodeja ja laitteen tiloja. Palvelusta löytyy valmiiksi useita malliratkaisuja eri yritystoimintojen käyttötarkoituksiin ja valmiudet rakentaa oman kuljetuspalveluiden tarpeisiin sopiva hallintajärjestelmä. (Azure IoT n.d.)

Kuvio 5 Azure IoT- palvelun esimerkki käyttönäkymä lämpötilajärjestelmän häiriötilanteesta (IoT in transportation and logistics n.d.)

5 Logistiikka-alan digitaalinen turvallisuus

Jotta logistiikkaketju olisi toimiva täytyy oikean tavaran olla oikeassa paikassa oikeaan aikaan. Nykyaikana logistiikkaketjulta vaaditaan tehokkuutta, sekä toimitusvarmuutta. Logistiikkaketjun toimiminen ympärivuorokautisesti edellyttää ulkoisten uhkien torjumista, joista yleisenä voidaan pitää kyberuhkia. Yritysten tietojärjestelmiä kehitetään jatkuvasti eteenpäin, mutta ne eivät vielä aina mahdollista sähköistä tiedonsiirtoa sidosryhmien välillä. Tietojärjestelmien eteenpäin kehittäminen perustuu täysin järjestelmän luotettavuuteen ja sen turvallisuuteen. Logistiikkayrityksillä on omat prioriteettinsa, jotka liittyvät kuljetustoimiin. Tällöin on hyvin yleistä, että he ostavat tarvittavat kyberturvallisuuspalvelut niitä tuottavilta yrityksiltä. Tämä takaa laadukkaan ja päivittyvän tuotteen, josta yrityksen ei tarvitse itse huolehtia. ParcelCall -projekti määrittää logistiikka-alan turvallisuusriskeihin lukeutuvan muun muassa: seurantajärjestelmien paikkatiedon hyödyntäminen fyysisten ryöstöjen tai vahingonteon toteuttamiseksi, tietojärjestelmiin murtautumisen perusteella haltuun saadut tuote- ja asiakastiedot ja liiketoiminnan estäminen häiritsemällä yrityksen verkkosivustoja tai muuta liiketoimintaa. Samaisessa projektissa annettiin kehotuksia

onnistuneen tietoturvan parantamiseksi, jakamalla muun muassa logistiikka-alan yrityksen asiakkaat pitkäaikaisiin sekä lyhytaikaisiin yhteistyökumppaneihin. Tällä rajataan sovellusten käyttäjät kahteen eri ryhmään, joilla on eri oikeudet tietojärjestelmiin. Molemmat käyttäjäryhmät pääsevät käsiksi tietoon erillisen suodatuksen läpi, jolloin heidän käsittelemä tieto voidaan rajata omistajayrityksen eli tässä tapauksessa kuljetusyrityksen toimesta. Poisrajattu tieto voi koskea esimerkiksi liiketoiminnan ja kuljetusverkoston yksityiskohtaisia ominaisuuksia. (Granqvist, Permala, Scholliers, Rauhamäki, Laakso & Varjola 2002.)

Parabhughate (2020) viittaa Stylianoun (2019) johtamaan The State of Logistics Technology Report -projektiin, jonka mukaan tärkeimmät logistiikka-alan tietotekniset kehityskohteet eivät ole pitäneet sisällään kyberturvallisuuden kehittämistä. Esimerkiksi kuljetus- ja varastonhallinta nähdään tärkeämpinä kehityskohteina. Tämä selittyy taloudellisella näkökulmalla, jonka mukaan yritykset haluavat panostaa toimintoihin, joista he saavat mahdollisimman paljon taloudellista hyötyä. Projektissa painotetaan myös logistiikka-alan yrityksien haluttomuutta vaikuttaa ja kehittää järjestelmiensä turvallisuutta. Haluttomuus näkyy muun muassa tietoturvajohtajan puutteesta (65 % palveluntarjoajayritykset, 57 % rahtiyhtiöt), joskin vain 21 % logistiikkayrityksistä uskoi tarvitsevansa tietoturvajohtajan. Noin joka toinen logistiikka-alan työntekijä kokee yrityksensä olevan huonosti valmistautunut havaitsemaan ja torjumaan suuremman luokan kyberhyökkäyksen. (Parabhughate 2020.)

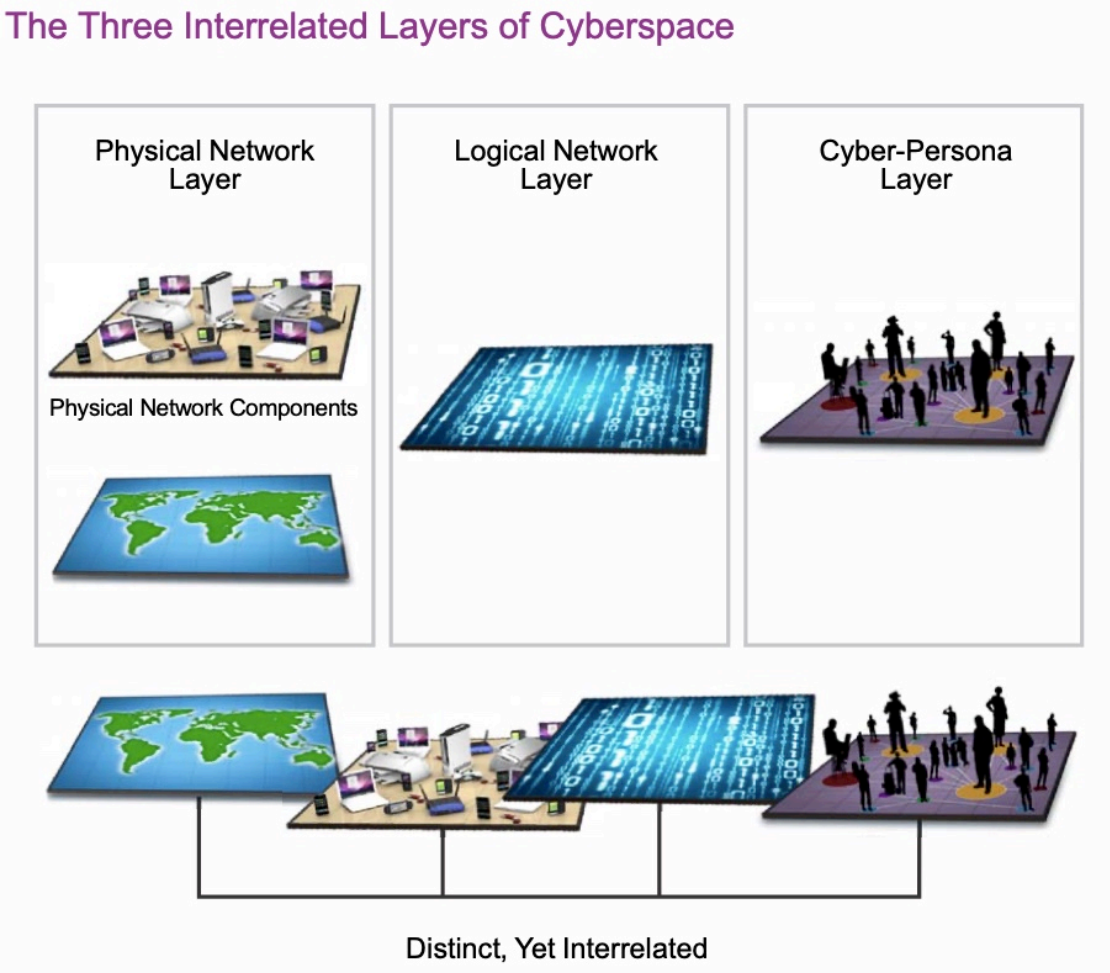
6 Kybervaikuttaminen logistiikkaa kohtaan

6.1 Kybertoimintaympäristö

Kybertoimintaympäristöllä tarkoitetaan laajaa tietojärjestelmien kokonaisuutta, johon myös fyysiset rakenteet ja toimijat kuuluvat. Ympäristön yksinkertaistamiseksi sen voidaan ajatella muodostuvan fyysisestä ja digitaalisesta maailmasta. Fyysinen maailma koostuu teknisten palveluiden infrastruktuurista ja digitaalinen maailma informaation liikkeestä tietojärjestelmien sisällä. Datan ja informaation tallentaminen,

siirto ja muokkaus teknologian avulla kuuluvat ympäristön ominaispiirteisiin. Tietojärjestelmät mahdollistavat kybertoimintaympäristön toiminnan ilman maantieteellisiä rajoja. Kybertoimintaympäristöjä ovat esimerkiksi toiminnanohjausjärjestelmät, kuljetus- ja logistiikkajärjestelmät ja finanssialan valuuttajärjestelmät. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.)

Kybertoimintaympäristö voidaan jakaa kerroksittain fyysiseen-, loogiseen- ja käyttäjäkerrokseen, jotka kukin pitävät sisällään eri ominaisuuksia. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.) Kerrokset ja niiden toimijat ovat eritelty kuviossa 6.



Kuvio 6 Kybertoimintaympäristön toisistaan riippuvaiset kerrokset (Joint Publication 3–12, 2018)

Fyysinen kerros (Physical Network Layer) sisältää fyysisiä komponentteja kuten palvelimia, tietokoneita ja päätelaitteita. Näiden lisäksi yleisen infrastruktuurin fyysiset reitit ja verkostot sekä maantieteelliset osat lasketaan mukaan fyysiseen kerrokseen. Maantieteellisillä osilla kuvataan fyysisten laitteiden tai toimintojen kuten sähkö- tai tietoverkkokaapelin sijaintia esimerkiksi rakennuksessa tai maan alla. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.)

Palvelut ja tietojärjestelmät, joita ei voi fyysisesti käsitellä kuuluvat loogiseen kerrokseen (Logical Network Layer). Ohjelmakoodit, tietopalvelut ja ohjelmistot ovat osa loogista kerrosta ja ne kommunikoivat fyysisten laitteiden esimerkiksi reitittimien tai tietokoneiden kautta. Tiedonsiirtoprotokollat, verkkoasetukset ja sovellukset ohjaavat keskustelua fyysisen kerroksen kanssa. Loogisella kerroksella pyritään varmistamaan tietoturvallisuus kybertoimintaympäristössä. Verkossa tapahtuva tiedustelutoiminta ja vaikuttaminen tapahtuvat loogisella tasolla, mutta siihen vaikuttaminen fyysisesti on hankalaa ilman puuttumista fyysisen kerroksen toimintoihin. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.)

Kybertoimintaympäristön inhimilliset toimijat kuuluvat käyttäjäkerrokseen (Cyber-Persona Layer). Ihmiset sulautuvat käyttäjäkerrokseen teknisillä toiminnoilla. Käyttäjäkerros yhdistää henkilöt ja ryhmät vuorovaikutukseen toisiensa kanssa tietoverkkojen kautta käyttämällä yksilöityjä käyttäjänimiä ja parametreja. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.)

Olemme tottuneet elämämme rakentuvan tietoverkkojen ympärille. Tarkastamme tulevan päivän sääennusteen verkosta, vastaamme sähköposteihin ja selaamme sosiaalista mediaa älypuhelimillamme. Kaiken tämän lisäksi yhteiskunnan kriittinen infrastruktuuri pyörii tietoverkkojen avulla, joka sitoo jokaisen palveluiden käyttäjän osaksi kybertoimintaympäristöä. Tämän perusteella jokaisen tulisi olla tietoinen siitä, miten kybertoimintaympäristössä menetellään. Valtion kyberturvallisuusstrategia ja Valtioneuvoston julkaisema selvitys kyberturvallisuuden nykytilasta käsittelevät kyberturvallisuutta kokonaisvaltaisesti valtion tasolla, kun taas Turvallisuuskomitean

Kodin kyberopas on suunnattu enemmän yksilötasolle tarjoamaan ohjausta jokapäiväiseen tietoturvallisuuden hallintaan. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.)

6.2 Kyberuhat

Kyberrikollisuus on kehittynyt viime vuosina laajaksi toimijaksi rikollisuuden parissa. Vuonna 2020 COVID-19 pandemian ottaessa koko maailman tietoisuuteensa yhä useammat kyberrikolliset käyttivät pandemiaa keinonaan vaikuttaa yhä useampiin kuluttajiin. Kyberuhaksi määritellään paheellinen tarkoitus tuhota tai muuten vahingoittaa tietojärjestelmää, tietoverkkoa tai päätelaitteita. Uhkia nykypäivän teknologian alalla ovat esimerkiksi kiristyshaittaohjelmat, laitteistoihin kohdistuvilla uhat, haavoittuvuuksien hyödyntäminen, henkilötietojen varastaminen, tietojenkalasteluhuijaukset palvelunestohyökkäykset sekä hyökkäykset liiketoimintaa kohtaan. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.)

Haittaohjelmat ovat erityisen hankalia uhkia, sillä nykyajan trendi on hyödyntää niitä laajaa toimialojen kirjoa vastaan. Uusia toimialoja maalitetaan hyökkäyksien kohteeksi mukaan lukien finanssiala sekä erinäiset hallinnolliset toimijat. Yrityksiin yhtenään kohdistuvat hyökkäykset altistavat koko sisäisen tietoverkon hattaohjelmille ja täten vaarantavat koko yrityksen tietopalvelut. Hyökkäyksiä kehitetään yhä useampiin päätelaitteisiin, joka selittyy älypuhelimien ja muiden laitteiden käytön lisääntymisellä. (Innola, Lehto, Limnéll, Pöyhönen, Rusi & Salminen 2017) Haittaohjelmat ujutetaan fyysisin tai teknisin keinoin uhrina olevan yrityksen tietojärjestelmiin. Taulukossa 2 esiintyy yleisimpinä pidetyt haittaohjelmat, joita ovat esimerkiksi kiristyshaittaohjelmat ja vakoiluohjelmat. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.)

Taulukko 2 Yleisimmät haittaohjelmat (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019, muokattu)

Virus (virus)	Haittaohjelma, jonka tarkoituksena on kopioida itseään ja levitä tietokoneesta toiseen. Esimerkiksi Brain, Iloveyou
Mato (worm)	Haittaohjelma, joka leviää tietokoneiden ja muiden päätelaitteiden välillä ilman käyttäjän toimia. Esimerkiksi Slammer, Conficker
Vakoiluohjelma (spyware)	Haittaohjelma, joka lähettää tietoa käyttäjän tiedostamatta ja ilman lupaa. Esimerkiksi DaVinci, FinFisher
Piilohallintaohjelma (rootkit)	Haittaohjelma asentuu uhritietokoneelle, kun hyökkääjä on saanut sen hallintaansa. Esimerkiksi Uroburos
Bottiverkko (botnet)	Saastuneista tietokoneista tai IoT-laitteista koottu verkko, jota käytetään erilaisten hyökkäyksien toteuttamiseen. Esimerkiksi Mirai
Troijanhevonen (trojans)	Harmittomaksi naamioitu haittaohjelma, joka todellisuudessa on vahingoksi uhrin tietokoneelle. Esimerkiksi Keymarble, Bandcall
Kiristyshaittaohjelma (ransomware)	Haittaohjelma salaa ja lukitsee päätelaitteen, sekä sen tiedostot ja vaatii maksusuoritusta niiden avaamiseksi. Esimerkiksi Petya, WannaCry

Kun pyritään vaikuttamaan tietyn yrityksen palvelujen toimintaan niin että niiden käyttäminen ja tietojen saatavuus estyy kokonaan puhutaan palvelunestohyökkäyksestä. Hyvin tyypillinen verkkosivujen lamaannuttaminen tapahtuu usein syöttämällä sivustolle niin paljon verkkoliikennettä, ettei se pysty käsittelemään kaikkea kerralla. Tämä näkyy kuluttajalle sivujen toimimattomuutena. Verkkoliikennettä voidaan työntää sivustolle kohdennetusti tai eri lähteistä hajautettuna palvelunestohyökkäyksenä, usein laajaa saastuneiden laitteiden verkkoa hyödyntämällä. Nykyään monet kotoa löytyvät älylaitteet ovat yhdistettävissä verkkoon ja huonon tietoturvan omaavat laitteet ovat vaarassa joutua mukaan väärin käytetyiksi muun muassa hajautettuun palvelunestohyökkäykseen. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.)

Suuri osa vaikuttamisesta teknisiin järjestelmiin tapahtuu tietoverkkojen välityksellä mutta on olemassa myös uhkatekijä, joka toimii teknisen järjestelmän kautta käyttäen hyväksi yksilön toiminnan inhimillisiä virheitä. Kybertoimintaympäristön käyttäjäkerrokseen kuuluvan henkilön manipulointia kutsutaan myös termillä social engineering. Se pyrkii vaikuttamaan uhriin tavalla, jonka perusteella hän suorittaa asioita omien etujensa vastaisin tuloksin. Erilaiset kalastelusähköpostiviestit, väärennetyt verkkosivustot ja huijauspuhelut ovat esimerkkejä käyttäjän manipuloinnista. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.) Taulukko 3 selventää tiedonkeruumenetelmiä, joilla pyritään vaikuttamaan käyttäjän toimintaan.

Taulukko 3 Yleisimmät käyttäjäpohjaiset tiedonkeruumenetelmät (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019, muokattu)

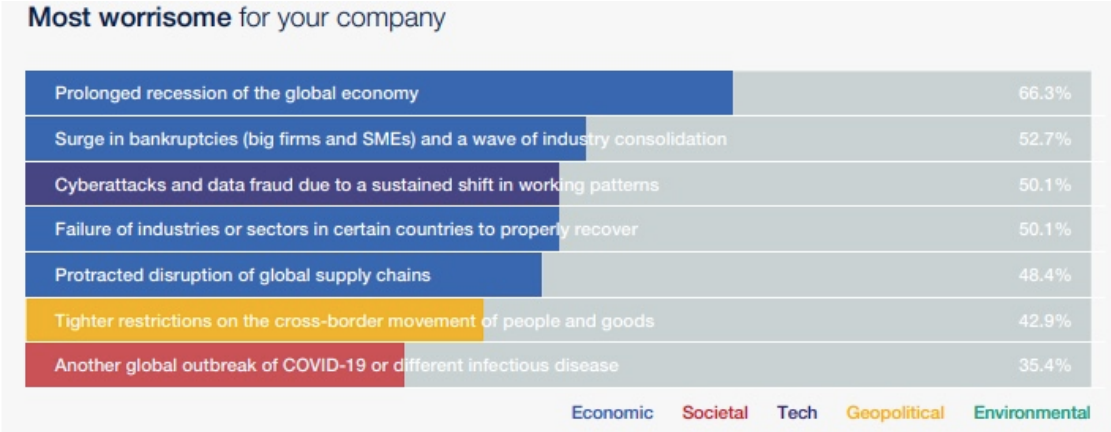
Huijausviesti tai verkkourkinta (phishing)	Sähköpostia ja vääriä tietoja käyttäen pyritään anastamaan luottamuksellisia tietoja, kuten henkilötietoja.
Kohdistettu huijausviesti (spear phishing)	Luottamuksellisten tietojen urkintaa sähköpostilla käyttäen vääriä tietoja kohdennettuna tiettyyn yritykseen tai yhteisöön.
Vaikutusvaltaisen henkilön huijaaminen (whaling)	Käyttäjämanipulointiin perustuvat hyökkäykset kohdistetaan vaikutusvaltaisiin henkilöihin muun muassa huijausviestein.
Saastuneet verkkosivut	Saastuneet verkkosivut voivat levittää eteenpäin haittaohjelmia sivustolla vierailleille.
Houkuttelu palkintojen avulla	Uhria houkutellaan erilaisten palkintojen avulla luovuttamaan esimerkiksi henkilötietojaan.
Huijauspuhelut	Uhria manipuloidaan huijauspuheluiden avulla luovuttamaan esimerkiksi henkilötietojaan.
Sosiaalisessa mediassa tapahtuvat huijaukset	Käyttäjiä manipuloidaan sosiaalisessa mediassa tai sen avulla osallistumaan esimerkiksi huijauksiin.

Kybertoimintaympäristössä haittaa tai vahinkoa aikaansaavat toiminnat ovat kyberhyökkäyksiä, jotka yhdessä muodostavat isomman toimintakokonaisuuden, kybe-

roperaation. Kyberhyökkäykset toistavat usein tiettyä kaavaa, jonka ymmärtääksemme tulee meidän keskittyä hyökkääjän toimiin ja tutustua kyberhyökkäyksen teknisen toteutuksen malliin. (Flyktman, Härmä, Laari, Timonen, Tuovinen 2019.) Laajaalaisesti tunnetun hyökkäysmallin on laatinut yhdysvaltalainen aseita, lentokoneita ja avaruustekniikkaa valmistava konserni Lockheed Martin. Seitsemän osainen vuonna 2011 julkaistu kyberhyökkäyksen vaiheistettu malli kuvaa hyökkääjän tunkeutumisvaiheita tietojärjestelmään murtautuessa. Se avaa hyökkäyksen tyypillisiä vaiheita kuten hyökkääjän taktiikoita, tekniikoita ja menettelytapoja. Lockheed Martinin malli on yksinkertainen toimiva ohjeistus hyökkäyksen kulkuun, mutta sen lineaarisuuden takia sitä seuraava turvallisuustoimija saattaa ajatella tilanteet liian yksinkertaisesti ja hypätä nopeasti johtopäätöksiin poissulkien muut vaihtoehdot. (The Cyber Kill Chain n.d.) Kyberhyökkäyksen vaiheittainen malli on Lockheed Martinin mukaan seuraavanlainen:

1. Tiedustelu ja tiedonkerääminen kohteena olevasta organisaatiosta. Tiedustelu tapahtuu keräämällä sähköpostiosoitteita ja muuta kriittistä tietoa kohteesta, joista saattaa olla hyötyä, esimerkiksi käytössä olevat järjestelmät ja niiden potentiaaliset haavoittuvuudet.
2. Aseistuksen rakentaminen. Hyökkääjä luo haittaohjelman, joka hyödyntää kohteen haavoittuvuuksia.
3. Kuljetus kohteeseen. Hyökkääjä käyttää sähköpostia, verkkoa tai USB-laitteita toimittaakseen haittaohjelman uhrin haltuun tai järjestelmään.
4. Aktivointi. Haittaohjelma aktivoituu itsestään tai toiminnan seurauksena ja se aloittaa uhrin haavoittuvuuksien hyödyntämisen.
5. Asennus. Haittaohjelma asentaa toiminnon, joka mahdollistaa hyökkääjän pääsyn uhrin järjestelmään etäyhteydellä.
6. Käsky ja hallinta. Haittaohjelma sallii hyökkääjälle pääsyn uhrin järjestelmään.
7. Toimenpiteet kohteessa. Kun hyökkääjällä on suora pääsy kohteeseensa, hän rupeaa toteuttamaan suunniteltua toimintaansa, joka voi olla esimerkiksi tiedostojen salaus maksusuoritteiden saamiseksi uhrilta sekä tietojen imurointi tai tuhoaminen. (Stanger 2020.)

Tietoverkkohyökkäykset logistiikka- ja kuljetusyrityksiin ovat Intelligence Fusionin (2020) mukaan tapahtuneet vuoden 2020 aikana suurelta osin käyttämällä erilaisia kiristyshaittaohjelmia sekä palvelunestohyökkäyksiä aiheuttaen häiriöitä yhtiöiden toimintoihin Kehittyneet jatkuvaksi uhaksi nähtävät kyberuhat kohdistavat yhä useampia hyökkäyksiä teollisien automaatiojärjestelmien tietoverkkoihin. Huolestuneisuutta on herännyt niin tietovarkauksia kuin infrastruktuurin haavoittuneisuutta kohtaan. Kotoaan tai muualta kuin työpaikalta käsin työskentelevät kokevat tarvitsevansa lähes yhtä vakaan ja luotettavan internetyhteyden kuin työpaikalla. (Harrington 2020.) Kuviosta 7 voidaan päätellä kyberhyökkäyksien olevan yksi suurimmista yrityksiä huolestuttavista uhista COVID-19-pandemian aiheuttamien tapahtumien vuoksi.



Kuvio 7 Kyberhyökkäyksien koettu uhka-arvo (World Economic Forum 2020)

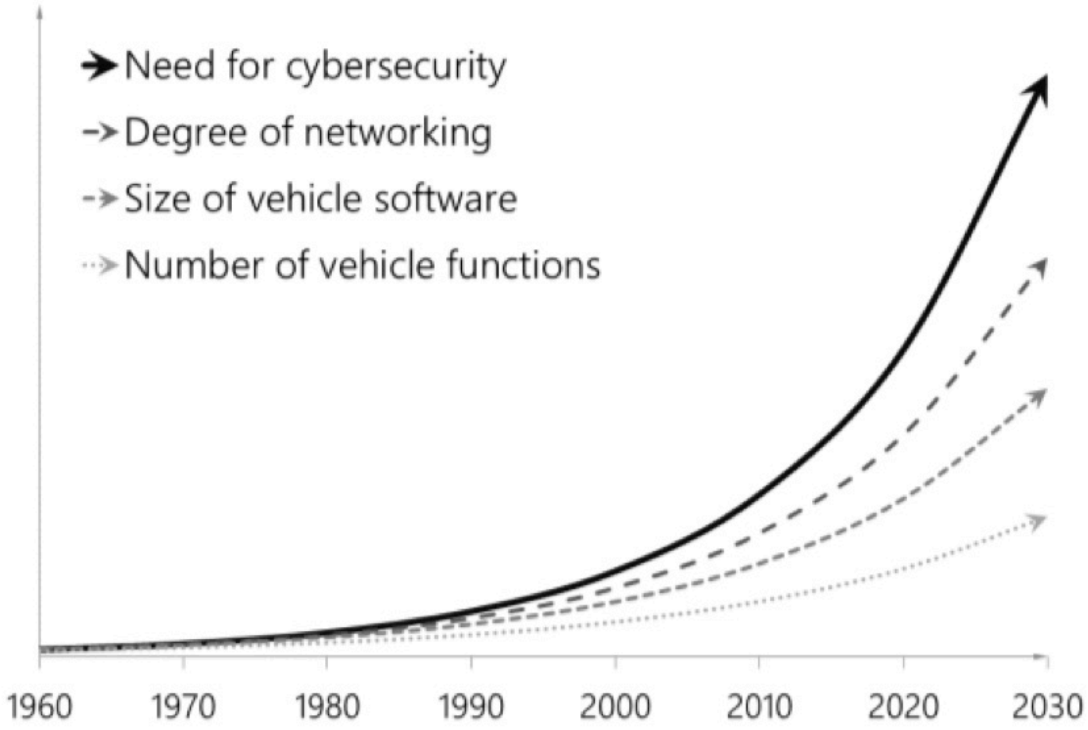
6.3 Vaikuttaminen kuljetuskalustoon

Raskaissa ajoneuvoissa lisääntyvä tietojärjestelmien määrä kasvattaa huomattavasti kyberhyökkäyksien riskiä kuljetus- ja logistiikka-alaa kohtaan. Raskaan kuljetuskaluston elektroniset ohjausjärjestelmät koostuvat suunnilleen 50 elektronisesta ohjausyksiköstä, jotka kommunikoivat keskenään käyttäen automaatioväyliä (CAN, Controller Area Network) mahdollistaen näin tiedonsiirron ilman isäntäkonetta. Autonomisen ohjauksen tehdessä tuloaan raskaaseen kalustoon kommunikointi ympäröivän

liikenteen ja tieverkoston kanssa lisääntyy. Tämän perusteella kyberturvallisuutta tulee käsitellä tärkeänä tekijänä yhdessä perinteisen liikenneturvallisuuden kanssa. Kuljetuskaluston teknologiajärjestelmät ovat laajempia verrattuna henkilöautoihin, jotka eivät sisällä seurantalaitteistoa tai datansiirtovälineitä. Kuljetuskalusto on liikkeellä ympärivuorokautisesti ja ne toimivat laajalla maantieteellisellä vyöhykkeellä, jolloin kuorma-autoon tehdyllä hyökkäyksellä on laaja vaikutus kuljetusyrityksen palveluihin. (Lambert & Wolf n.d.)

Autonominen ohjaus tulee mullistamaan henkilö- ja rahtiliikenteen tulevina vuosikymmeninä. Teslan kehittämä Autopilot-järjestelmä on jo antanut viitteitä siitä miten autonomista ohjausta voidaan hyödyntää henkilöliikenteessä ja sama koskee kuljetuspalveluita. Useat autonomisten rekkojen kehittäjät ovat väläytelleet onnistumisia kuljetusalalla kuten Yhdysvaltalainen TuSimple, joka on yksi merkittävien läpimurtojen tekijöistä. San Diegossa pääkonttoriaan pitävä kuljetusyritys on ryhtynyt kehittämään autonomista tekniikkaa, aikomuksenaan yhdistää se merkittävän strategisen osaamisen kanssa. TuSimple on ryhtynyt yhteistyöhön kuorma-autovalmistaja Navistarin sekä kuljetusjätti UPS:n (United Postal Service) kanssa suunnitelmanaan rekkojen täysin autonominen ajo varastojen välillä. Nykyiset testit Arizonassa ja Texasissa suoritetaan kuitenkin vielä niin sanottuna valvottuna autonomisena kuljetuksena, jolloin ihminen on läsnä rekan hytissä ajoneuvoyhdistelmän ajaessa itse. Autonominen toiminta vaatii paljon tekniikkaa toimiakseen, jolloin erilaiset anturit hoitavat suuren osan ympäristön tarkkailusta syöttäen lukemaansa informaatiota ajotietokoneeseen, joka päättää ajoneuvon ohjaamisen toimista. Antureita on kameroiden, tutkien ja optisen valotutkan muodossa. Raskaan kuljetuskaluston automatisointi kaupalliseen liikenteeseen voi olla nopeampaa henkilöautoliikenteeseen verrattuna, jonka syynä on lähinnä raskaan kaluston kuljetusreittien yksinkertaisuus ja moottoriteiden käyttö mahdollistaen ennakoivamman ja helpomman navigoinnin määränpäähän. Rekkojen korkeus ja suuri koko helpottaa antureiden havainnointikykyä ympäristön suhteen sekä teknisten järjestelmien suunnittelua ja sijoittamista kaluston rakenteisiin. (Ackerman 2021.) Autonomisten kuljetusjärjestelmien yleistyessä on tärkeää keskittyä teknisten järjestelmien suojaamiseen uhilta. Pelkästään nykyinen kuljettajan ohjaama kuljetusmuoto sisältää lukuisia tietojärjestelmiä, joihin on mahdollista vaikuttaa kyberhyökkäyksillä ja vaarantaa näin kuljetuskokonaisuus. Kaupallisen liikenteen

kuljetusmuotojen kehittymisen nähdään kasvavan voimakkaasti seuraavan vuosikymmenen aikana tarkoittaen tietojärjestelmien määrän kasvua raskaissa kuljetusajoneuvoissa. Polttoainetehokkuuden, kuljetusten turvallisuuden ja kuljetuskaluston hallinnan parantaminen merkitsee yhä enemmän tulevaisuudessa ja vaatii näin ollen useamman tietojärjestelmän per ajoneuvoyhdistelmä. Tietojärjestelmien lisääntyminen kasvattaa digitaalisten rajapintojen määrää, jolloin tarve kyberturvallisuudelle moninkertaistuu kuten kuviosta 8 voi nähdä. (Lambert & Wolf n.d.)



Kuvio 8 Kuljetusmuotojen digitalisaation seurauksena tapahtuva järjestelmien toimintojen monimutkaistuminen (Lambert & Wolf n.d.)

6.4 Kyberhyökkäystapaukset logistiikan alalla

6.4.1 Eurooppa

Konglomeraatti A. P. Møller-Mærsk A/S joutui vakavan kybervaikuttamisen kohteeksi kesäkuussa 2017. Kyseessä on maailman suurin rahtilaivavarustamo, joka operoi

maailmanlaajuisesti yli 130 maassa ja työllistää lähes 80 000 henkilöä. NotPetya niminen haittaohjelma pysäytti sekä aiheutti merkittäviä viivästyksiä satamien rahtitoimintaan New Yorkissa, Mumbaissa ja kymmenissä muissa maissa ympäri maailman. Haittaohjelma lukitsi suurimman osan Maersk:n tietojärjestelmistä ja näin esti pääsyn niiden hallinnointiin. Yrityksen koko viestintäjärjestelmä täytyi lopulta sulkea haittaohjelman eristämiseksi. (Sham 2019) NotPetya käyttää alun perin Yhdysvaltojen kansallisen turvallisuusviraston NSA:n (National Security Agency) kehittämää Eternalblue- tietoturva-aukkoa. Se hyödyntää haavoittuvuuksia SMB (Server Message Block) protokollaa käyttävissä Windows-järjestelmissä. NotPetyan toiminta tapahtuu manipuloimalla massamuistilaitteen (MBR, Master Boot Record) osiota, josta BIOS (Basic Input Outboot System) hankkii käyttöjärjestelmän latauskoodin. Hyökkäyksessä uhrin käyttöjärjestelmän alkuperäinen MBR korvataan hyökkääjän muokkaamalla datalla, jonka jälkeen tietokone määrätään käynnistymään uudelleen asetetun aikamäärän jälkeen. Uudelleenkäynnistymisen yhteydessä hyökkääjän asettama koodi salaa yksittäisen tietokoneen tiedostot vaatien maksusuoritusta hyökkääjän asettamaa siirtokanavaa pitkin sekä levittää itseään käytössä olevassa tietoverkossa eteenpäin hyödyntäen Eternalblue- haavoittuvuutta. (Paganini 2017.)

Sveitsiläis-Italialainen maailman toiseksi suurin kontteja kuljettava rahtiyritys Mediterranean Shipping Company joutui kyberhyökkäyksen kohteeksi huhtikuussa 2020. Hyökkäys häiritsi hetkellisesti yhtiön palveluita maailmanlaajuisesti, mutta se saatiin eristettyä nopeasti palvelimiin yhtiön pääkonttorissa Genevessä, jolloin merkittävämpää vahinkoa ei päässyt syntymään. Mediterranean Shipping Companyn verkkosivut olivat poissa käytöstä useiden päivien ajan. Geneven pääkonttorin palvelimiin kohdistunut hyökkäys toteutettiin kiristyshaittaohjelmalla, joka salasi useita tiedostoja tavoitteenaan maksusuorituksien vaatiminen rahtiyritykseltä. (Goud n.d.)

CMA CGM S.A rahtiyritys kohtasi kyberhyökkäyksen palveluitaan vastaan syyskuussa 2020. Palvelimien heikkouksia kartoittavan haittaohjelman takia ranskalaisen yrityksen oli pakko sulkea verkkopalveluitansa ja ohjata asiakkaitansa eri kanavien käyttöön. CMA CGM myönsi järjestelmämurron tapahtuneen, mutta sillä ei ollut vaikutusta yhtiön viestintätoimintoihin tai satama- ja rahtitoimintaan. (Shipping industry

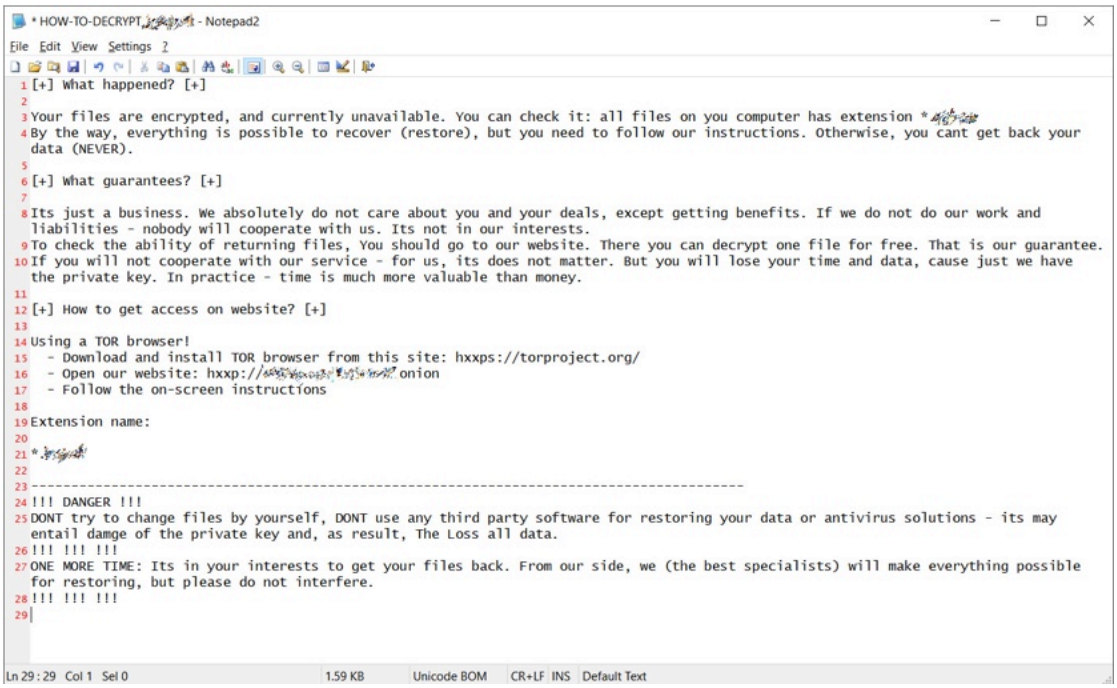
hit by multiple cyber attacks 2020.) Ragnar Locker- tyypin kiristyshaittaohjelmahyökkäyksen tarkoituksena oli varastaa kriittistä informaatiota ja lukita käyttöjärjestelmät vaatien niiden avaamisesta maksua. Ragnar Locker on tietojen salausohjelma, joka hyödyntää Microsoft:n Windows käyttöjärjestelmää. Haittaohjelman manuaalista aktivointia edeltää kattava tiedustelu ja ennakkoon suoritettuja tehtäviä uhrin tietoverkon sisällä kuten arkaluontoisten tietojen kerääminen ja niiden kopiointi hyökkääjän palvelimelle. Näitä tietoja kannustimena käyttäen hyökkääjä antaa aikamäärän uhrille, jonka loppuessa hyökkääjä julkaisee arkaluontoiset tiedot tai materiaalin jos maksusuoritusta ei ole tehty. (Tavares 2020.)

6.4.2 Yhdysvallat

Konglomeraatti COSCO ajautui kybervaikuttamisen kohteeksi vuonna 2018 kun yhtiön Yhdysvaltojen toimipaikkojen tietoverkkoja vastaan hyökättiin. COSCO:n Long Beachin satamassa sijaitsevaa rahtiterminaalia vastaan toteutettu kiristyshaittaohjelmahyökkäys aikaansai hallitun tietoverkkojen osittaisen alasajon, jonka aikana paikalliset sähköposti- ja telekommunikaatioverkot olivat poissa käytöstä. Rahtiliikenteeseen hyökkäyksellä ei ollut vaikutusta, mutta kiristyshaittaohjelman eristäminen pelkästään yhtiön Yhdysvaltojen tietoverkkoihin ei onnistunut ja ohjelma levisi lopulta laajemmalle Etelä-Amerikkaan. Ainakin Argentiinan, Brasilian, Chilen, Kanadan, Panaman, Perun ja Uruguayn toimipisteet joutuivat kiristyshaittaohjelman vaikutuksen alaisiksi. Sähköposti- ja telekommunikaatioverkot Etelä-Amerikassa jouduttiin myös sulkemaan ja COSCO päätyi antamaan ilmi lukuisia julkisia sähköpostiosoitteita, joiden kautta kommunikaatio asiakkaiden ja yhtiön välillä onnistui. (Paganini 2018.)

Yhdysvaltalainen logistiikkayritys Forward Air Corporation kärsi 7.5 miljoonan dollarin tappiot kyberhyökkäyksen aiheuttamasta kiristyshaittaohjelmasta joulukuussa 2020. Yhtiö joutui sulkemaan kaikki tietojärjestelmänsä, jonka seurauksena tietoverkkoliikenne asiakkaidensa kanssa keskeytyi. (Cimpanu 2021.) Cimpanun (2021) mukaan Kingston (2020) varmistaa Tennesseessa sijaitsevaan yrityksen toimintojen kärsivän valtavia ongelmia, kun kuljettajat ja työntekijät eivät päässeet sähköisesti käsiksi tarvittaviin dokumentteihin, joita tarvittiin kuorman tullauskäsittelyihin valtioiden vä-

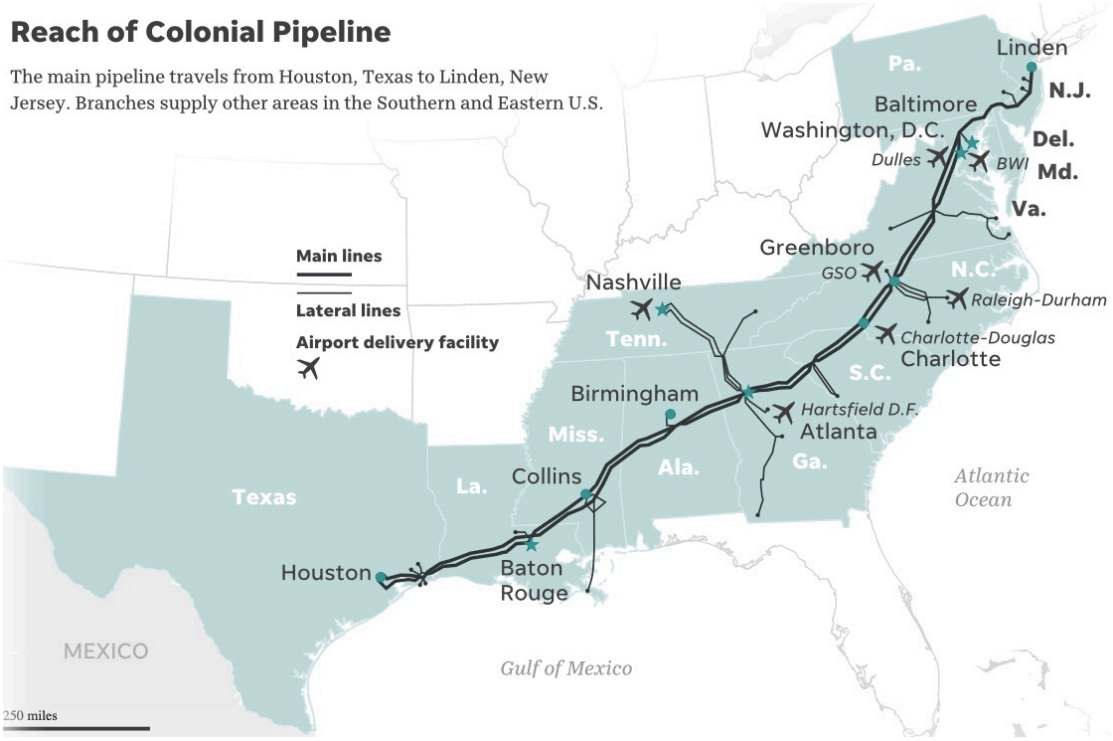
lillä. Forward Airin mukaan hyökkäyksestä palauduttiin onnistuneesti, mutta Yhdysvaltojen arvopaperi- ja pörssikomission SEC:n (United States Securities and Exchange Commission) tekemästä dokumentista sekä muista tappioista johtuva taloudellinen häviö osoittaa sen miksi yhä useammat yritykset panostavat ennaltaehkäisevään toimintaan hyökkäyksien estämiseksi kuin jälkiseurauksien mittavaan käsittelyyn. (Cimpanu 2021.) Cimpanu (2021) mainitsee Abramsin (2020) käsittelevän kirityshaittaohjelman toteutusta Forward Airin tapauksessa ja paljastavan kyseessä olevan uudenlainen Hades-kiristyshaittaohjelma. Hades luo tekstitiedoston lunnasvaatimuksesta salatessa uhrin järjestelmätiedostoja, muistuttaen REvil-kiristyshaittaohjelmaryhmän käyttämää tiedostoa. Tekstitiedostossa tarjotaan myös henkilökohtainen URL-osoite, joka ohjaa uhrin Tor-sivustolle esittäen informaatiota hyökkäyksestä ja Tox-viestipalvelun osoitteen, jonka kautta hyökkääjiin voi olla yhteydessä. Kuvio 9 esittää lunnasvaatimuksen uhrin vastaanottamasta viestistä, jossa paljastuu järjestelmätietojen salaus. (Cimpanu 2021.)



Kuvio 9 Hades-kiristyshaittaohjelman lunnasvaatimus (Abrams 2020)

Yksi Yhdysvaltojen suurimmista bensiinin ja muiden polttoaineiden kuljetusputkistosta joutui kyberhyökkäyksen kohteeksi toukokuussa 2021. Colonial Pipeline -yhtiön kuljetusputkisto kuljettaa bensiini-, diesel- ja lentokonepolttoainetta Texasista New

Yorkin asti. Yhdysvaltojen itärannikon käyttämästä polttoaineesta noin 45 % kuljetetaan Colonial Pipelinen Texas-New York putkistossa. Colonial Pipelinen maantieteellisesti tavoittama alue näkyy kuviossa 10. Viranomaisten mukaan kyseessä oli Yhdysvaltojen historian suurin kyberhyökkäys öljynkuljetusalaa kohtaan. Uutistoimisto Reutersin mukaan hyökkääjät saivat haltuunsa yli 100 gigabittiä dataa Colonial Pipelinen pilvipalvelusta. Colonial Pipeline joutui sulkemaan polttoainekuljetusputkistonsa hyökkäyksen takia 7.5.2021 ja sai otettua tietojärjestelmänsä uudelleen käyttöön vasta 12.5.2021. Kuljetusputkisto avattiin hiljalleen tämän jälkeen. Hyökkäyksen aiheuttama polttoainepula ja pidentyneet polttoainetoimituksien rajoitukset saattavat nostaa polttoaineiden hintojen entisestään, kunnes talous elpyy koronaviruksenpandemian aiheuttamasta sokista. Yhdysvaltain keskusrikospoliisi FBI (Federal Bureau of Investigation) vahvisti hyökkäyksen takana olleen ammattirikollisjärjestö DarkSide. (Beard, Loehrke, Padilla & Petras 2021.)



Kuvio 10 Colonial Pipelinen maanteiteellisesti tavoittama alue Yhdysvaltojen itäosassa (Beard, Loehrke, Padilla & Petras 2021)

Uutistoimisto Washington Post kertoo ulkoisen tutkijan onnistuneen selvittämään tapahtumien kulun sekä varastetun informaation sisältävän palvelimen sijainnin ja ilmoittaneen asiasta FBI:lle, jotka olivat yhteydessä kyseisen palvelimen operaattoriin. Palvelimen operaattori sai eristettyä palvelimen, jonka tuloksena hyökkääjät saattoivat menettää pääsyn varastettuihin tiedostoihin kokonaan. Hyökkäyksessä käytettiin Pankovin (2021) mukaan kiristyshaittaohjelmaa, joka oli DarkSiden käsialaa. Molemmilla Windows- ja Linux-käyttöjärjestelmillä operoiva kiristyshaittaohjelma käyttää vahvaa salausta, jonka murtaminen ilman oikeaa salausalgoritmin avainta on mahdotonta. (Pankov 2021.)

6.4.3 Aasia

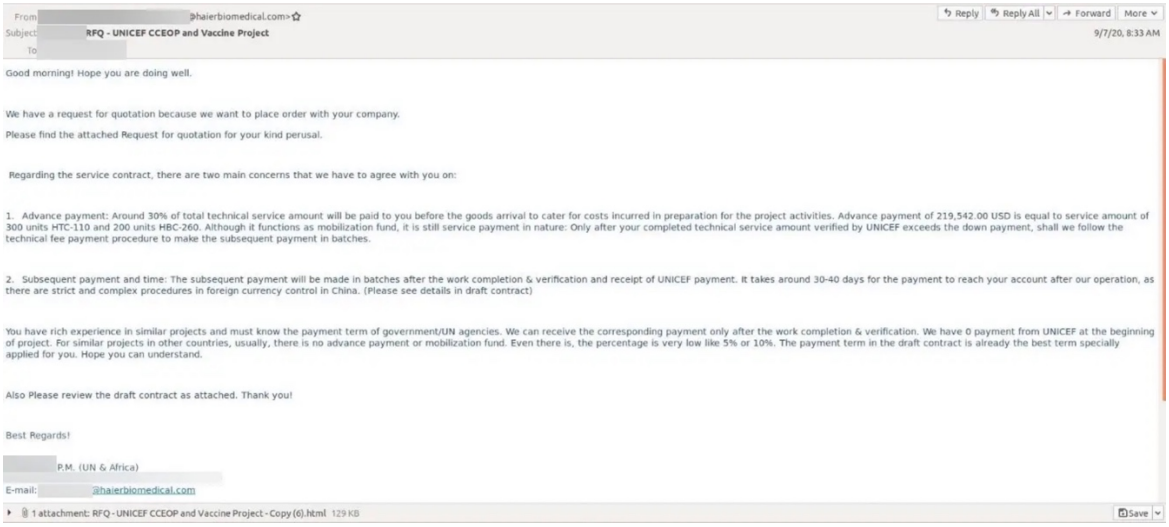
Intian kuljetussektoriin vuoden 2021 alussa kohdistuneet kyberhyökkäykset olivat Kiinan valtion tukemia vaikuttamisiskuja (After power, Chinese hackers target transport sector 2021). After power, Chinese hackers target transport sector -artikkelissa viittaaman Intian elektroniikka- ja tietotekniikkaministeriön alla operoivan tietoturvaloukkausten ennaltaehkäisytiimin CERT-In:n (Indian Computer Emergency Responce Team) luoman muistion mukaan CERT-In on havainnut hyökkäysten olevan kohdennettua tunkeutumista Intian kuljetussektoria kohtaan mahdollisena tavoitteenaan tiedustelu ja kybervakoilun suorittaminen. Tunnetut kybertoimijat APT15/K3yChang, APT27/Emissary Panda, APT41/Barium, APT101 StonePanda, RedEcho ja Wnnti groups ovat vaikuttaneet useisiin intialaisiin kuljetusalan yhtiöihin. Muun muassa Intian valtion liikenne ja infrastruktuurialojen asiantuntijayritys RITES (Rail India Technical and Economic Services), Intian rautateidentietojärjestelmien keskus CRIS (Centre for Railways Information Systems) sekä Intian rahtikuljetuksien kehityksestä ja turvallisuudesta vastuussa oleva DFCCIL (Dedicated Freight Corridor Corporation of India) joutuivat kaikki kyberhyökkäyksien kohteiksi. Hyökkääjät käyttivät monipuolisia vaikutuskeinoja, johon kuuluivat muun muassa kohdistettu huijausviestintä (spear phishing), haittaohjelmien tahaton lataus tietokoneelle (Drive via Download) ja tunnettujen haavoittuvuuksien hyödyntäminen tietojärjestelmien sisälle pääsemiseksi. Tietoturvaloukkausten ennaltaehkäisytiimi CERT-In on informoinut kuljetussektorin alaisia yrityksiä Intiassa tehostamaan kyberturvallisuusinfrastruktuuriaan välittömästi. (After power, Chinese hackers target transport sector 2021.)

Kybervaikuttaminen Maerskia kohtaan vuonna 2017 aloitti uuden kyberuhkien aikakauden. Samana vuonna esitetyt vaikuttamiset Yhdysvaltojen presidentinvaaleihin, WannaCry -haittaohjelma, sekä aieimmin mainittu NotPetya nostivat kyberrikollisuuden vahvasti maailman tietoisuuteen. Maerskiin kohdistuneen hyökkäyksen takia kuljetusala joutui haluamattaan kybervaikuttamisen keskiöön. (Sharrock 2018.)

6.4.4 Tapausesimerkki kyberhyökkäyksestä COVID-19-pandemian aikana kuljetus- ja logistiikka-alaa kohtaan

IBM:n (International Business Machines Corporation) kaupallisen turvallisuuden tutkimusryhmä Security X-Force perusti COVID-19-pandemian alkaessa uhkatiedusteluun keskittyvän ryhmän, jonka tehtävänä on selvittää COVID-19-pandemiaan liittyviä kyberuhkia, joista on riskianalyysin perusteella merkittävä uhka niille logistiikkaorganisaatioille kenen vastuulla on COVID-19 rokotteen toimitusketjun toteutus ja hallinta (Incident response and threat intelligence services n.d). Ryhmän analyysin perusteella havaittiin maailmanlaajuinen huijauskampanja kohdennettuna COVID-19 rokotteiden kylmäketjua hallinnoiviin toimijoihin. COVID-19 rokotteiden säilytyksessä on huomioitava matalan lämpötilan jatkuva ylläpito, jolloin rokotteen ihanne säilytyslämpötila saavutetaan. Kylmäketjun turvallinen hallinta tarkoin säädellyissä olosuhteissa on elintärkeä edellytys rokotteen turvalliselle käytölle. Vaikuttaminen logistiikkaorganisaatioihin alkoi Security X-Force:n mukaan syyskuussa 2020 ulottuen kuuteen maahan ja kohdistuen organisaatioihin, jotka tukivat rokotusliittouma Gavin, UNICEF:n (Yhdistyneiden kansakuntien lastenrahasto) ja muiden kumppanien yhteistyössä kehittämää alustaa kylmäketjulaitteiden optimisointiseksi nykystandardien tasolle. 2015 perustettu CCEOP (Cold Chain Equipment Optimization Platform) on 400 miljoonan dollarin yhteisprojekti, joka levittäytyy viiden vuoden aikavälille tavoitteenaan päivittää nykyiset rokotteiden kylmäketjujärjestelmät 56 maassa varmistaakseen rokotteiden turvallisen säilyvyyden. (Frydrych & Zaboeva 2020.) Pelkästään COVID-19 rokotteille parannusta järjestelmien päivittämisellä ei haeta vaan projektin päämäärä on mitoitettu toimimaan auttavana tekijänä myös muiden nopeasti leviävien vaarallisten tautien ehkäisemiseen tarkoitettujen rokotteiden ja muiden lääkkeiden perille kohdemaahan saamisessa (Keeping vaccines safe through the last mile

of their journey 2020). Uhriorganisaatioiden vastaanottamien tietojenkalasteluviestien lähettäjänä esiintyi kylmäketjujen jakelutoiminnoista vastaava työntekijä kiinalaisesta Haier Biomedical- yrityksestä. Haier Biomedical toimii mukana CCEOP-projektissa yhtenä yrityskumppanina, joten pääteltävissä on hyökkääjän halunneen hyötyä Haier Biomedicalin statuksesta, sillä yritys on maailman ainoa täysimittaisten kylmäketjukokonaisuuksien toimittaja ja suuri vaikuttaja CCEOP-projektissa. Tietojenkalasteluviestien aiheena ollut kysely CCEOP-projektin tarjouspyyntöihin liittyen sisälsi pahanlaatuisen HTML-linkin (Hypertext Markup Language), joka avautuessaan pyysi käyttäjän tunnistetietoja tiedostojen tarkastelua varten. Tietojenkalasteluviesti kuviossa 11 sisältää HTML-linkin ja lisätietoa valheellisesta tilauksesta. HTML-linkin käyttäminen sähköpostiviestissä tunnistetietojen kyselyä varten poissulki hyökkääjän perusteen erillisen huijausverkkosivuston luomiselle. Kohdeuhreina olleisiin toimijoihin kuuluivat Euroopan komission verotuksen ja tullliliiton pääosasto DG TAXUD (Directorate-General for Taxation and Customs Union), sekä muita maailmanlaajuisia organisaatioita energian-, ohjelmistokehityksen-, teollisuuden- ja tietoturvallisuuden sektoreilta levittäytyen ympäri Eurooppaa sekä Aasiaa. Energiasektorin aurinkopaneelien valmistusyrityksiin kohdistetulla tietojenkalastelulla pyrittiin vaikuttamaan negatiivisesti COVID-19 rokotteiden kylmäsäilytykseen käytettävien rokotekaappien tarvitseman sähkön tuottamien aurinkopaneelien valmistukseen. Eteläkorealainen ja saksalainen ohjelmistokehitysyritys joutuivat niin ikään tietojenkalasteluviestien kohteeksi. Saksalaisen yrityksen tiedettiin tukevan lääkevalmistajia, eri kuljetusalan toimijoita, biotekniikan yrityksiä sekä navigointipalveluihin sähkökomponentteja tuottavia yrityksiä. Korkeassa asemassa hankinnan, myynnin, rahoituksen ja tietotekniikan parissa olevat työntekijät, joilla oli suuri todennäköisyys olla mukana vaikuttamassa oman yrityksensä suunnitelmiin COVID-19 rokotteiden kylmäketjun tukemiseen joutuivat tiedonkalastelusähköpostien kohteiksi. (Frydrych & Zaboeva 2020.)


From [redacted]@haierbiomedical.com>
Subject: RFQ - UNICEF CCEOP and Vaccine Project
To [redacted]
Reply | Reply All | Forward | More
9/7/20, 8:33 AM

Good morning! Hope you are doing well.

We have a request for quotation because we want to place order with your company.

Please find the attached Request for quotation for your kind perusal.

Regarding the service contract, there are two main concerns that we have to agree with you on:

1. Advance payment: Around 30% of total technical service amount will be paid to you before the goods arrival to cater for costs incurred in preparation for the project activities. Advance payment of 219,542.00 USD is equal to service amount of 300 units HTC-110 and 200 units HBC-260. Although it functions as mobilization fund, it is still service payment in nature: Only after your completed technical service amount verified by UNICEF exceeds the down payment, shall we follow the technical fee payment procedure to make the subsequent payment in batches.

2. Subsequent payment and time: The subsequent payment will be made in batches after the work completion & verification and receipt of UNICEF payment. It takes around 30-40 days for the payment to reach your account after our operation, as there are strict and complex procedures in foreign currency control in China. (Please see details in draft contract)

You have rich experience in similar projects and must know the payment term of government/UN agencies. We can receive the corresponding payment only after the work completion & verification. We have 0 payment from UNICEF at the beginning of project. For similar projects in other countries, usually, there is no advance payment or mobilization fund. Even there is, the percentage is very low like 5% or 10%. The payment term in the draft contract is already the best term specially applied for you. Hope you can understand.

Also Please review the draft contract as attached. Thank you!

Best Regards!

[redacted] P.M. (UN & Africa)
E-mail: [redacted]@haierbiomedical.com

1 attachment: RFQ - UNICEF CCEOP and Vaccine Project - Copy (6).html 129 KB
Save

Kuvio 11 COVID-19 rokotteen toimitusketjuun liittyvien organisaatioiden työntekijöille lähetetty tietojenkalasteluviesti (Frydrych & Zaboeva 2020)

Microsoftin uhkatiedusteluun keskittyvä ryhmä kertoo arvioineensa huijausviesti-kampanjan tarkoituksena olleen uhriyrityksen kirjautumistietojen haltuunotto ja niiden hyödyntäminen myöhempänä ajankohtana luvattomassa järjestelmäkäytössä. Hyökkääjät voisivat saada toiminnallaan pääsyn tietoihin COVID-19 rokotteeseen liittyvästä viestinnästä, sen suunnitelluista jakelumenetelmistä aina valtiollisen infrastruktuurin hyödyntämiseen lähetyksien toimittamisessa julkisen terveydenhuollon haltuun. Hyökkääjän saamat kirjautumistiedot mahdollistaisivat myöhemmän verkkovakoilun ja luottamuksellisen tiedon keräyksen tulevaisuuden kyberoperaatioita varten. (Frydrych & Zaboeva 2020.)

7 Digitaalisen turvallisuuden parantaminen

Kyberuhat kehittyvät yhtä lailla teknologian kehittyessä. Analyytikot haluavat kehittää järjestelmiään uusin innovaatioin, mutta valitettavasti uhkatoimijat tiedostavat tämän ja muuntavat toimintojaan yhä vaarallisemmiksi ja tehokkaimmiksi. Yhä useampien elektroniikkalaitteiden yhdistäminen tietoverkkoon kasvattaa mahdollisten laitekaappauksien määrää käytettäväksi esimerkiksi hajautetussa palvelunestohyökkäyksessä. Vaikka kyberuhkat eivät ole uusi ilmiö, viime vuosikymmenien voimakas

digitalisaation kasvu on tuonut uhkien ja hyökkäyksien haittavaikutukset lähemmäs ihmisten jokapäiväistä elämää. Kyberuhilla voidaan nykypäivänä vaikuttaa kriittisesti valtioiden infrastruktuuriin ja yhteiskunnan sektoreihin, jotka tuovat erittäin vakavat poikkeustilanteet yhä todennäköisemmäksi tulevaisuudessa.

Digitaalinen turvallisuus rakentuu aina sisäisten järjestelmien ympärille riippumatta yrityksestä tai sen toimialasta. Logistiikka-alalla näiden järjestelmien suojaaminen on tehokas tapa rakentaa yritykselle suojamuuri digitaalisia uhkia vastaan. Tätä pidetäänkin yhtenä konkreettisimmista toiminnoista, joita yrityksen tulisi kehittää, sillä tällä on suora vaikutus yrityksen tietojen turvaamiseen. Huomioitavaa on työntekijöiden kouluttaminen tasolle, mikä takaa mahdollisimman hyvän suojan inhimillisiä virheitä vastaan. Työntekijöiden tulisi olla tietoisia siitä, miten heidän toimintansa vaikuttaa yrityksen järjestelmiin ja toimintoihin mahdollisen tietojenkalastelun tai kyberhyökkäyksen sattuessa. On tärkeää kouluttaa työntekijä toimimaan oikein tilanteessa, jossa hän havaitsee epäilyttävän linkin sähköpostiviestissä tai epämääräisen URL-osoitteen. Pelkästään yrityksen omien työntekijöiden kouluttaminen ei ole riittävää kattavan suojauksen saavuttamiseksi. Kyberturvallisuussuunnitelmassa tulee varmistua alihankkijoiden ja muiden yhteistyökumppaneiden tietoturvallisuustason olevan yhtä kattavalla tasolla kuin asiakasyrityksen. Yhteistyökumppanilta olisi hyvä pyytää yksityiskohtainen turvallisuusarviointi, josta selviää yrityksen tietoturvallisuustaso erillisen tietoturvallisuusyrityksen suorittamana. Oman IT-osaston käyttäminen arvioinnin suorittamiseen on myös mahdollista. Arvioinnista tulisi selvitä esimerkiksi mitä tietoturvatyökaluja yhteistyökumppaneilla on käytössä, miten työtekijöiden pääsyä rajoitetaan eri järjestelmiin sekä minkälainen ohjelmistojen päivitys on käytössä. Myös kybervakuutuspalveluita olisi hyvä harkita, mutta ainoastaan tukemaan voimassa olevia kyberturvallisuustoimia. Kybervakuutuksella tarkoitetaan palvelua, jolla turvataan yrityksen liiketoiminnan jatkuvuus tilanteessa, jossa yrityksen tietoverkkopalveluihin on päästy vaikuttamaan. Sen tarkoitus on täydentää tietoturvapalveluita, ei korvata niitä. Ennen kybervakuutuksen harkitsemista, tulisi yrityksen omat tietoturvapalvelut olla lähtökohtaisesti ajan tasalla. (Cybersecurity in Logistics: How to Protect Your Supply Chain from Cyber-Attacks 2020.)

Yksinkertaisimmat kyberturvallisuustoiminnot, joita logistiikka- ja kuljetusyrityksien tulisi käyttää turvaamaan toimintansa pitävät sisällään esimerkiksi viruksen torjunta-ohjelmistot, palomuurit, salatut yhteydet, suojaukset tietovuodoille sekä vahvat suojaukset erilaisia kiristyshaittaohjelmia vastaan. Edellä mainittujen lisäksi täytyisi kiinnittää huomiota vahvaan roskapostien suodatukseen, jolla pyritään estämään tietojenkalasteluyritykset ja mahdolliset kiristyshaittaohjelmien levitykset. (Cybersecurity in Logistics: How to Protect Your Supply Chain from Cyber-Attacks 2020.)

8 Tutkimustulokset

Tutkimustuloksissa keskitytään vastaamaan tuloksien perusteella opinnäytetyössä esitettyihin tutkimuskysymyksiin. Työn tutkimuskysymyksiä oli kolme, joista ensimmäisen tavoitteena oli selvittää kuljetus- ja logistiikkaketjuihin kohdistuvia kyberuhkia. Kuljetus- ja logistiikkaketju on moniosainen järjestelmä, jonka ohjaaminen ja hallinta on toteutettu pääosin tietojärjestelmiä käyttäen avaten näin mahdollisuuden kybertoimijoille vaikuttaa tietojärjestelmiä vastaan. Erilaisia kyberuhkia on monenlaisia, mutta merkittävimmän uhan kuljetusalaa kohtaan aiheuttavat tiedonkalastelu- ja huijausviestikampanjat sekä kiristyshaittaohjelmat. Teknologian kehittyessä ja digitalisaation pohjustaessa jokapäiväistä elämäämme palvelut siirtyvät yhä nopeammin verkkoon kyberuhkien vaikutusalueelle. Hyökkääjien kannalta on tuottoisaa hyödyntää tilannetta käyttämällä tiedonkalastelu- ja huijausviestikampanjoita käyttäjätietojen huijaamiseksi. Näitä tietoja käyttämällä nyt tai tulevaisuudessa voidaan päästä käsiksi kuljetusyrityksen järjestelmiin ja hyödyntää saatavilla olevaa informaatiota rikollisiin tarkoituksiin. Mahdollisuus on myös niin sanotun takaoven (backdoor, itsenäinen ohjelma tai komento) jättämistä uhrin järjestelmään, joka mahdollistaa luvattoman pääsyn järjestelmään ilman tietoturvatodennuksen käyttöä. Tutkimuksessa todettiin hyökkääjien käyttävän tiedonkalastelu- ja huijausviestikampanjoita myös kiristyshaittaohjelmien apuna uhrin kiristämiseksi. Tällöin hyökkääjä on saanut tiedonkalastelulla haltuunsa järjestelmän kirjautumistietoja, joiden avulla asennetaan kiristyshaittaohjelma uhriyrityksen järjestelmään. Hyökkääjät suosivat myös sähköpostitse lähetettävää kiristyshaittaohjelmaa naamioituna haitattomaksi tiedostoksi,

jonka uhrin halutaan avaavan. On selvää, että kiristyshaittaohjelmat ovat yksi käytetyimmistä hyökkäysmenetelmistä sen monimuotoisuuden ansioista. Se tarjoaa hyökkääjälle laajan spektrin käyttömahdollisuuksia ja on erittäin vaarallinen oikein kohdistettuna.

Toisen tutkimuskysymyksen tavoitteena oli selvittää miten kuljetus- ja logistiikkaketjuihin liittyviä kyberuhkia voidaan välttää. Kuljetus- ja logistiikkaketjujen kyberuhkien välttämiseksi tulee tarkastella ketjujen kyberturvallisuutta kahdessa osiossa. Ensimmäisessä osiossa käsitellään hallinnan tietojärjestelmiä, joiden voidaan olettaa toimivan normaaleissa toimistotiloissa ja verkoissa. Kyberrikollisten käynnistämät tiedonkalastelu- ja huijausviestikampanjat pyrkivät huijaamaan työntekijää, jolloin henkilöstön kouluttaminen tietoturvapoikkeumien havainnointiin on erityisen tärkeää. Voidaan olettaa nykypäivän standardien valossa yrityksen käytössä olevien tietojärjestelmien olevan valmiiksi hyvin suojattuja ja varmennettuja (viruksen torjuntaohjelmistot, sähköpostin roskapostisuodatukset, salatut yhteydet), joten niiden käsittely on ei ole oleellista. Huomiota tulisi kohdistaa IT-palveluiden kyberturvallisuuteen sijoittamalla omaan kyberturvallisuusosastoon, jota johtaa tietoturvajohtaja. On myös harkittava mahdollisen kybervakuutuksen hankkimista. Toinen osio käsittelee kuljetusmuotojen manipulointia kyberhyökkäyksillä. Nykyajan raskas kalusto sisältää lukuisia tietoteknisiä järjestelmiä, joilla tarkkaillaan kaikkea kuorman tilasta kuljetusreitin ruuhkaisuuteen. Tekniset laitteet lisääntyvät jatkuvasti ja pian raskas kalusto integroidaan autonomiseen kuljetusverkkoon, jolloin ihminen ei enää hallitse lähetyksen kuljetusta. Kuljetuskalusto on täynnä tietoteknistä laitteistoa ja periaatteena voidaan pitää, että jokainen verkossa kiinni oleva tekninen laite voidaan hakkeroida ja ottaa haltuun. Tämä vaarantaa kuljetusketjun vakaville turvallisuusriskeille, jotka vaikuttavat tavalla tai toisella negatiivisesti yrityksen talouteen. Mahdollisuutena on esimerkiksi kuljetuksien sabotointi ja tuhoaminen (muun muassa lämpötilasäädellyt tuotteet), jolloin kuluja tulee menetetystä kuormasta tai ajoneuvojen tietojärjestelmien lamaannuttaminen, jolloin toimimattomilla ajoneuvoilla ei voida kuljettaa lähetyksiä, joka vaikuttaa niin ikään negatiivisesti yrityksen tulokseen. Kuljetusmuotojen tietojärjestelmiin vaikuttamalla aiheutetaan katkoksia kuljetusketjujen hallittavuuteen, joka näkyy häiriöinä kuljetusten perille saamisessa.

Kolmas tutkimuskysymys käsitteli kyberturvallisuuden merkitystä yrityksille kokonaisuudessaan. Yrityksien menestyminen perustuu toimivan liiketalouden ympärille ja liiketalouden on pidettävä valuutta virtaamassa yrityksen sisällä. Valuuttavirtojen ehtyminen vaarantaa koko yrityksen toimivuuden, joten toiminnot tulee turvata sen mukaan, ettei mikään pysty vaikuttamaan negatiivisesti kassavirtaan. Fyysinen turvallisuus nähdään itsestään selvyytenä. Ovet pidetään lukittuina ja hälytysjärjestelmä päällä, kun tiloissa ei työskennellä. Vähemmän tärkeämpänä esittäytyy tietojärjestelmien turvallisuus eli kyberturvallisuus, jonka kehittäminen tulisi nähdä merkittävänä sijoituksena yrityksen tulevaisuuteen. Poiketen fyysisen turvallisuuden toimintatavoista, kyberturvallisuudella suojattavat järjestelmät ovat hyödynnettävissä aina kun yrityksen tietojärjestelmät ovat toiminnassa eli periaatteessa vuorokauden ympäri. Hyökkääjä pystyy tarkkailemaan ja tiedustelemaan kohdetta ilman riskiä kiinnijäämisestä ja hyökkäyksen toteutus voi onnistua kohdeyrityksen huomaamatta hyökkäystavasta riippuen. Nykyajan tietojärjestelmien verkottuneisuuden takia yritykset ovat suuremmassa vaarassa kuin koskaan joutua kybervaikuttamisen kohteeksi ja tämä näkyy yritysten yhä suuremmassa kiinnostuksessa kyberturvallisuuspalveluita kohtaan. Voidaan siis olettaa kyberturvallisuuden olevan erittäin merkityksellinen osaalue yrityksien kehittämissuunnitelmissa.

9 Pohdinta & Johtopäätökset

Opinnäytetyön tarkoituksena oli selvittää kuljetus- ja logistiikkayrityksien kyberturvallisuutta sekä sen uhkia ja merkitystä yrityksille. Tutkimuksen tulokset vastasivat esitettyihin tutkimuskysymyksiin tarkasti. Kyberturvallisuus ja siihen liittyvät uhkatekijät ovat kehittyneet viime aikoina merkittävästi. Tekniset toiminnot ja teknologiat ovat kehittyneet yleisesti tietotekniikan alalla, joka on mahdollistanut molemmin puolisen kehityksen tietoturvan toimijoiden keskuudessa. Tuloksien perusteella kuljetus- ja logistiikkayrityksien tulee kehittää kyberturvallisuuttaan jatkuvasti pysyäkseen verkkorikollisten vaikuttamattomissa nyt ja tulevaisuudessa.

Kyberturvallisuuden hallinta vaatii yrityksien henkilöstöltä huomattavaa osaamista sekä valppautta tunnistaa ja estää mahdollisten digitaalisten uhkatekijöiden aiheuttamat vaaratilanteet. Nykyajan tietoturvauhat omaavat niin monipuoliset jakelualustat, että työntekijöiltä vaaditaan erityistä tarkkaavaisuutta. Tietoturvauhat voivat naamioitua USB-muistitikussa sijaitsevaksi harmittomaksi tiedostoksi, liitteeksi tärkeältä näyttävässä sähköpostiviestissä tai autenttiseksi websivustoksi esittäytyväksi tahoksi, joka todellisuudessa onkin huijaussivusto.

Aiheena kuljetus- ja logistiikkayrityksien kyberturvallisuus sekä niiden uhat ja merkitykset yrityksille oli erittäin laaja ja sen rajaus oman ja toimeksiantajan kuvauksen mukaiseen muotoon oli haastavaa, mutta onnistuin rajaamaan aiheen tiiviiksi sekä monipuoliseksi kokonaisuudeksi. Vaikka kuljetus- ja logistiikka-alojen toimintaa ei koulutuksessani käsitelty, pystyin muodostamaan kokonaiskuvan aloista etsimällä tietoa niiden toiminnasta ja yhdistämällä kyberturvallisuuden tietämystäni kattavaksi kokonaisuudeksi. Työssä halusin tuoda esille merkittävimmät kuljetus- ja logistiikkaketjujen uhkatekijät sekä niihin liittyvät kyberturvallisuuden teknologiat. Tavoitteena oli mahdollisimman laaja hyöty työn toimeksiantajalle JYVSECTEC:lle sekä muille kyberturvallisuuden ja kuljetus- ja logistiikka alan yrityksille.

Lähteet

Abrams, L. 2020. Trucking giant Forward Air hit by new Hades ransomware gang. Artikkeli Bleeping Computer:n sivustolla. Viitattu 9.5.2021. https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-hit-by-new-hades-ransomware-gang/

Ackerman, E. 2021. This Year, Autonomous Trucks Will Take to the Road With No One on Board. Artikkeli IEEE Spectrum:n sivustolla. Viitattu 10.5.2021. https://spectrum.ieee.org/transportation/self-driving/this-year-autonomous-trucks-will-take-to-the-road-with-no-one-on-board

After power, Chinese hackers target transport sector. 2021. Artikkeli The Hindu BusinessLine:n sivustolla. Viitattu 15.5.2021. https://www.thehindubusinessline.com/news/national/after-power-chinese-hackers-target-transport-sector/article34125502.ece

Azure IoT. N.d. Artikkeli Microsoft Azure:n sivustolla. Viitattu 8.5.2021. https://azure.microsoft.com/en-us/overview/iot/

Beard, S., Loehrke, J., Padilla, R. & Petras, G. 2021. US gas prices rise as Colonial Pipeline reopens after ransomware attack. Artikkeli Usa Today:n sivustolla. Viitattu 15.5.2021. https://eu.usatoday.com/in-depth/graphics/2021/05/10/colonial-pipeline-closed-hackers-ransomware-gasoline-jet-fuel-cybercrime/5019625001/

Cimpanu, C. 2021. Trucking company Forward Air said its ransomware incident cost it $7.5 million. Artikkeli ZDNet:n sivustolla. Viitattu 9.5.2021. https://www.zdnet.com/article/trucking-company-forward-air-said-its-ransomware-incident-cost-it-7-5-million/

Churchill, T. 2018. Why Cyber Security is Very Important in the Modern World. Artikkeli The Info Center:n sivustolla. Viitattu 3.2.2021. https://www.thecenteratmdc.org/cyber-security-important-modern-world/

Cybersecurity in Logistics: How to Protect Your Supply Chain from Cyber-Attacks. 2020. Artikkeli Evans Distribution Systems:n sivustolla. Viitattu 21.3.2021. https://www.evansdist.com/cybersecurity-in-logistics/

Dahlberg, T., Korpela, K., Lammi, M., Lankinen, M., Mikkonen, K. & Nykänen, L. 2019. Hajaantuneesta hajautettuun: Dokumenteista dataan, toimijakeskeisyydestä yhteentoimiviin ekosysteemeihin. Liikenne- ja viestintäministeriön julkaisu. Viitattu 1.5.2021. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161898/LVM_2019_12.pdf

Delcuvellerie, D. 2018. Tracking of aircraft in distress using the cospas-sarsat system. Julkaisu 2018 SpaceOps konferenssissa. Viitattu 29.4.2021. https://arc.aiaa.org/doi/pdf/10.2514/6.2018-2343

Digitaalisuus logistiikassa. N.d. Logistiikan Maailman sivusto. Viitattu 1.5.2021. https://www.logistiikanmaailma.fi/aineistot/logistiikkaa-lukiolaisille/digitaalisuus-logistiikassa/

Dong, Z. 2013. The technical conditions of modern logistics. Shandong yliopiston tutkimus. Viitattu 20.4.2021. https://file.scirp.org/pdf/JSS_2013110716071005.pdf

Flyktman, J., Härmä, K., Laari, T., Timonen, J. & Tuovinen J. 2019. # kyberpuolustus: kyberkäsikirja Puolustusvoimien henkilöstölle. Maanpuolustuskorkeakoulun julkaisu. Viitattu 3.5.2021. https://www.doria.fi/bitstream/handle/10024/173254/%23kyberpuolustus%20verkko%20%28interaktiivinen%20pdf%29%20%28002%29.pdf?sequence=1&isAllowed=y

Frelinger, D., Frost, G., Fossum, D., Lachow, I., Pace, S., Pinto, M. & Wassem, D. 1995. The global positioning system: assessing national policies. Critical Technologies Institute:n julkaisu. Viitattu 5.5.2021. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR614/MR614.pdf

Frydrych, M & Zaboeva, C. 2020. IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain. Artikkeli Security Intelligence:n sivustolla. Viitattu 9.5.2021. https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/

Galileo's contribution to the MEOSAR system. N.d. Julkaisu Euroopan komission sivustolla. Viitattu 29.4.2021. https://ec.europa.eu/growth/sectors/space/galileo/sar/meosar-contribution_en

Goud, N. N.d. Mediterranean Shipping Company MSC hit by a Cyber Attack. Artikkeli Cybersecurity Insiders:n sivustolla. Viitattu 7.5.2021. https://www.cybersecurity-insiders.com/mediterranean-shipping-company-msc-hit-by-a-cyber-attack/

Granqvist, J., Permala, A., Scholliers, J., Rauhamäki, H., Laakso, J. & Varjola, M. 2002. Tavarakuljetusten seuranta TASKU. VTT Rakennus- ja yhdyskuntatekniikan tutkimusraportti. Viitattu 24.4. https://www.vttresearch.com/sites/default/files/julkaisut/muut/2002/tasku_raportti.pdf

Harrington, D. 2020. The rising risk of cyber attacks on logistics and transport. Artikkeli Intelligence Fusion:n sivustolla. Viitattu 3.5.2021. https://www.intelligence-fusion.co.uk/insights/resources/intelligence-reports/the-rising-risk-of-cyber-attacks-on-logistics-and-transport/

Haverinen, I. 2020. Tulevaisuuden joustava toimitusketju taipuu myös poikkeustilanteisiin. Artikkeli Midagonin sivustolla. Viitattu 30.4.2021. https://www.midagon.com/tulevaisuuden-joustava-toimitusketju-taipuu-myos-poikkeustilanteisiin/

How Logistics Began. 2019. Artikkeli Filuet:n sivustolla Viitattu 21.3.2021. https://filuet.com/how-logistics-began/

Incident response and threat intelligence services. N.d. Incident response and threat intelligence services -palvelun esittely. Viitattu 9.5.2021. https://www.ibm.com/security/services/ibm-x-force-incident-response-and-intelligence

Innola, E., Lehto, M., Limnéll, J., Pöyhönen, J., Rusi, T., & Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston kanslian julkaisu. Viitattu 2.5.2021. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160233/Suomen_kyberturvallisuuden_nykytila,__tavoitetila_ja.pdf?sequence=1

IoT in transportation and logistics. N.d. Artikkeli Microsoft Azure:n sivustolla. Viitattu 8.5.2021. https://azure.microsoft.com/en-us/overview/iot/industry/transportation-and-logistics/

Joint Publication 3-12. 2018. Cyberspace Operations. Viitattu 3.5.2021 https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Keeping vaccines safe through the last mile of their journey. 2020. Viitattu 9.5.2021. https://www.unicef.org/supply/stories/keeping-vaccines-safe-through-last-mile-their-journey

Kingston, J. 2020. News Alert: Forward Air suffering significant IT outage. Viitattu 9.5.2021. https://www.freightwaves.com/news/news-alert-forward-air-suffering-significant-it-outage

Kuljetukset. N.d. Logistiikan Maailman sivusto. Viitattu 1.5.2021. https://www.logistiikanmaailma.fi/kuljetus/

Laadullinen tutkimus. 2015. Jyväskylän yliopisto. Viitattu 12.5.2021. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus

Lambert, R. & Wolf, M. N.d. Hacking Trucks – Cybersecurity Risks and Effective Cybersecurity Protection for Heavy-Duty Vehicles. Viitattu 10.5.2021. http://www.marko-wolf.de/files/WoLa17_Hacking_Trucks.pdf

Logistiikka ja toimitusketju. N.d. Logistiikan Maailman sivusto. Viitattu 29.4.2021. https://www.logistiikanmaailma.fi/logistiikka/logistiikka-ja-toimitusketju/

Merikuljetus. N.d. Merikuljetusosion johdantoesitys Logistiikan Maailman sivustolla. Viitattu 1.5.2021. https://www.logistiikanmaailma.fi/kuljetus/merikuljetus/

Microsoft logistics team gains supply chain visibility using Azure IoT Central. 2020. Viitattu 8.5.2021. https://customers.microsoft.com/en-us/story/777252-microsoft-consumer-goods-azure

Mitä on logistiikka? N.d. Logistiikan Maailman sivusto. Viitattu 21.3.2021. https://www.logistiikanmaailma.fi/aineistot/logistiikkaa-lukiolaisille/mita-on-logistiikka/

Overview. N.d. Yritysesittely JYVSECTEC:n sivustolla. Viitattu 11.5.2021. https://jyvsectec.fi/about/overview/

Paganini, P. 2017. CSE CybSec ZLAB Malware Analysis Report: NotPetya. Artikkeli Security Affairs:n sivustolla. Viitattu 8.5.2021. https://securityaffairs.co/wordpress/63081/malware/zlab-malware-analysis-report-notpetya.html

Paganini, P. 2018. Ransomware attack against COSCO spread beyond its US network to Americas. Artikkeli Security Affairs:n sivustolla. Viitattu 8.5.2021. https://securityaffairs.co/wordpress/74941/malware/cosco-ransomware-attack-followup.html

Pankov, N. 2021. How Colonial Pipeline managed its ransomware attack. Artikkeli Kaspersky:n sivustolla. Viitattu 15.5.2021. https://www.kaspersky.com/blog/pipeline-ransomware-mitigation/39907/

Parabhughate, A. 2020. Cybersecurity for transport and logistics industry. Infosys:n julkaisu. Viitattu 21.3.2021. https://www.infosys.com/services/cyber-security/documents/transport-logistics-industry.pdf.

Sham, M. 2019. Cybersecurity concerns within the logistics industry. Artikkeli More Than Shipping:n sivustolla. Viitattu 21.3.2021. https://www.morethanshipping.com/cybersecurity-concerns-within-the-logistics-industry/

Sharrock, J. 2018. Cybersecurity and the threat to logistics. Cyber Citadel:n julkaisu. Viitattu 21.3.2021. https://www.cybercitadel.com/docs/Cyber-Security-and-the-Threat-to-Logistics-A.pdf

Shipping industry hit by multiple cyber attacks. 2020. Artikkeli Reuters Events:n sivustolla. Viitattu 7.5.2021. https://www.reutersevents.com/supplychain/supply-chain/shipping-industry-hit-multiple-cyber-attacks

Stanger, J. 2020. Think Like a Hacker: 3 Cybersecurity Models Used to Investigate Intrusions. Artikkeli Comptia:n sivustolla. Viitattu 5.5.2021. https://www.comptia.org/blog/think-like-a-hacker-3-cybersecurity-models-used-to-investigate-intrusions

Stojić, G., Tanackov, I. & Tepić, J. 2011. Ancient logistics – historical timeline and etymology. Novi Sad:n yliopisto. Viitattu 21.3.2021. https://www.researchgate.net/publication/283863501_Ancient_logistics_-_historical_timeline_and_etymology.

Stylianou, N. 2019. The State of Logistics Technology Report 2019. Eye For Transport:n julkaisu. Viitattu 21.3.2021. https://eloqua.eft.com/LP=25040?extsource=logisticstechreportwerc

Tapaninen, U. N.d. Logistiikan tulevaisuuden näkymät. Helsingin kaupungin yrityspalveluiden julkaisu. Viitattu 30.4.2021. https://www.uudenmaanliitto.fi/files/23522/Ulla_Tapaninen_Logistiikan_tulevaisuuden_nakymat.pdf

Tavares, P. 2020. Ragnar Locker malware: what it is, how it works and how to prevent it Malware spotlight. Artikkeli Infosec:n sivustolla. Viitattu 7.5.2021. https://resources.infosecinstitute.com/topic/ragnar-locker-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/

The Cyber Kill Chain. N.d. Artikkeli Lockheed Martin:n sivustolla. Viitattu 6.5.2021. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Tutkimuksen toteuttaminen. 2010. Jyväskylän yliopisto. Viitattu 15.5.2021. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/tutkimusprosessi/tutkimuksen-toteuttaminen

Vihavainen, T. 2020. Satelliittipaikannuksen nykytila ja kehitysnäkymät. Artikkeli Traficomin sivustolla. Viitattu 26.4.2021. https://www.traficom.fi/fi/satelliittipaikannuksen-nykytila-ja-kehitysnakymat

Williams, T. 2020. Military logistics in the ancient world. Artikkeli Tom Williams Author:n sivustolla. Viitattu 5.4.2021. https://tomwilliamsauthor.co.uk/military-logistics-in-the-ancient-world/

World Economic Forum. 2020. COVID-19 Risks Outlook A Preliminary Mapping and Its Implications. World Economic Forum:n julkaisu. Viitattu 3.5.2021. http://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf