

Miksi harjoitella?

Cyber Europe kyberturvallisuusharjoitus

27.3.2026

European Logistics Institute, ELI - Xamk

Yksikön johtaja Vesa Vainio



**ELI - European
Logistics Institute**

Toimintaympäristön muutosvoimat



ELI - European
Logistics Institute

Toimitusketjujen haavoittuvuudet



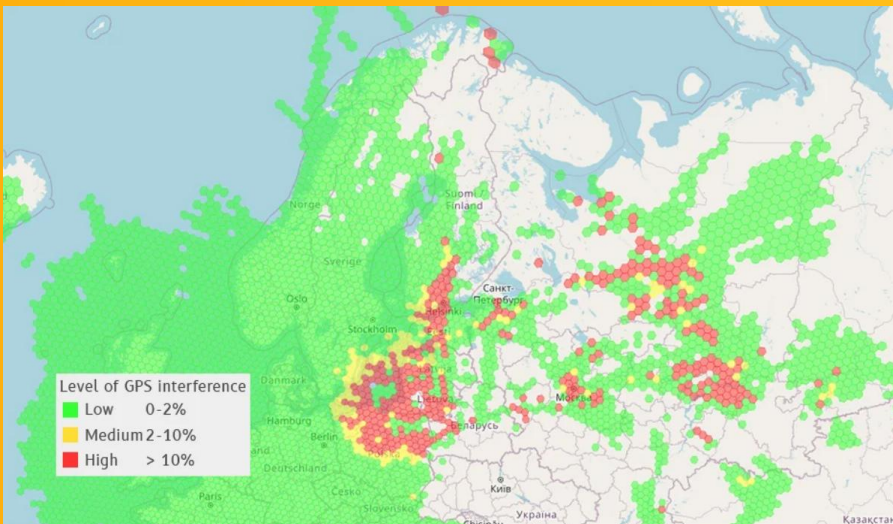
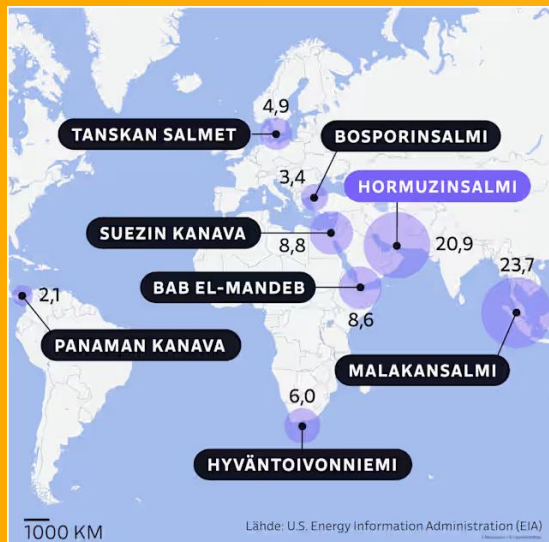
ELI - European
Logistics Institute

Merikuljetusriippuvuus ja kriittiset reitit

Merikuljetusten merkitys : Suomessa jopa 95 % tavaroista kulkee meriteitse, mikä tekee merikuljetuksista kriittisen osan ulkomaankauppaa.

Navigointijärjestelmien häiriöt: GPS- ja GNSS-häirinnät voivat vaarantaa alusten reitit ja aiheuttaa merkittäviä riskejä kuljetusketjuille. Varjolaivasto.

Riskit toimitusketjuille: Satamien sulkemiset, työmarkkinahäiriöt ja kyberhyökkäykset voivat nopeasti lamauttaa merikuljetukset.

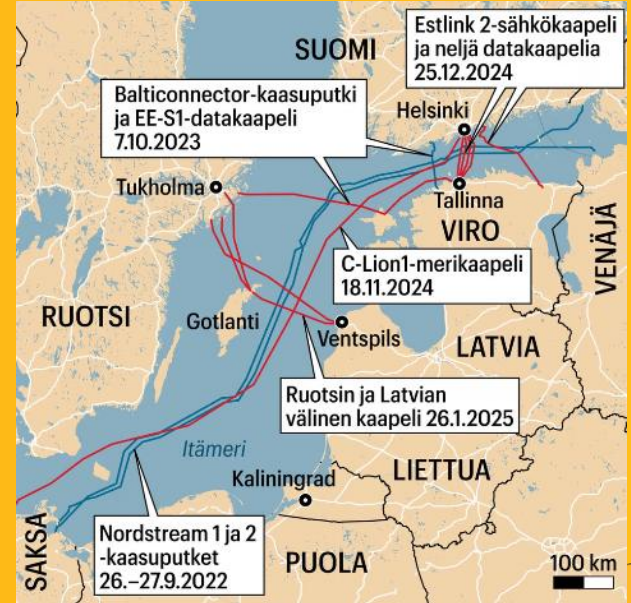


Satama- ja väyläinfrastruktuuriin liittyvät riskit

Navigointivirheet GNSS-häirinnän vuoksi: GNSS-häirinnän lisääntyminen kasvattaa alusten navigointivirheiden riskiä satamissa ja väylillä.

Kyberuhat satamainfrastruktuurissa: Satamien teknologinen riippuvuus altistaa ne kyberhyökkäyksille, joihin EU vastaa turvallisuusstandardeilla.

Vedenalaisen infrastruktuurin riskit: Vedenalaisen infrastruktuurin vauriot ovat kasvava riski Itämeren alueen väylillä.



Kuva is.fi 28.1.2025



ELI - European
Logistics Institute

Toimenpiteitä toimitusketjujen vahvistamiseen

Navigointijärjestelmien turvallisuus: Vaihtoehtoisten navigointimenetelmien kehittäminen ja henkilöstön koulutus GNSS-häiriöihin parantavat toimitusketjujen turvallisuutta.

Kyberturvallisuuden vahvistaminen: EU-satamastrategian mukaiset yhteiset turvallisuusstandardit ja teknisten haavoittuvuuksien korjaus parantavat satamien kyberturvallisuutta.

Toimitusketjujen resilienssi: Monilähteiset hankintaketjut ja varastointimallit lisäävät joustavuutta ja vähentävät riskejä häiriö- ja kriisitilanteissa.

Yhteistyö ja koordinaatio: Virallisten toimijoiden ja yritysten yhteistyö on olennainen osa toimitusketjujen turvallisuuden kokonaisvaltaista varmistamista.



ELI - European
Logistics Institute

Miksi harjoitella?

Harjoittelu muuttaa tietämisen osaamiseksi ja valmiudeksi toimia käytännössä.

1. Osaaminen syvenee ja vakiintuu
2. Teoriasta käytäntöön
3. Virheiden tekeminen turvallisesti
4. Itseluottamus ja toimintavarmuus kasvavat
5. Yhteistyö
6. Valmius häiriötilanteisiin



PAPU Kyber 25 – harjoituksen tavoitteet



- harjoittaa PAIKP kyberosien yhteistoimintaa sataman ja vesilaitosten kanssa, puolustuksen valmisteluihin ml. yt- suunnitelman tekoon ja toimintaan kyberpuolustuksessa.
- harjoittaa satamatoimijoita ja vesilaitoksia toimimaan eri kybertilanteissa
- harjoittaa kybertilannekuvan muodostamista ja jakamista

Harjoitus liittyy Karelian Stronghold 25 paikallispuolustusharjoitukseen sekä E-S AVI Kaakko 25 valmiusharjoitukseen

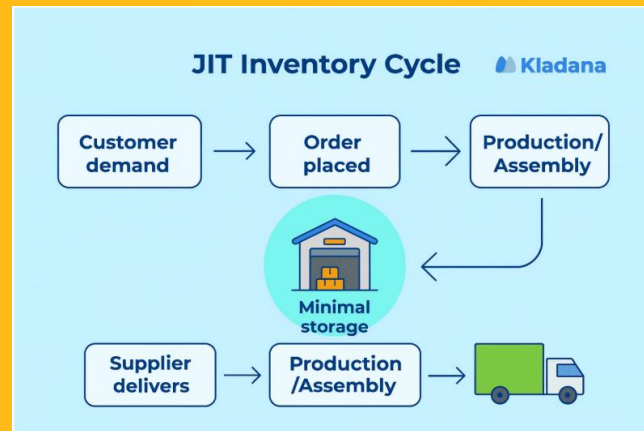


European
cs Institute

Mitä se voisi olla pk-yrityksen näkökulmasta?

Pk-yrityksen näkökulmasta harjoittelu on ennen kaikkea riskienhallintaa, liiketoiminnan turvaamista ja arjen sujuvuuden varmistamista.

1. Liiketoiminnan sujuvuuden varmistaminen
2. Virheet eivät kaada koko yritystä
3. Ajansäästö ja tehokkuus arjessa
4. Henkilöstön sitouttaminen
5. Asiakkaiden ja kumppaneiden luottamus (kilpailuetu)
6. Ei vaadi mittavia investointeja
7. Harjoittelu paljastaa kehityskohdat



ELI - European
Logistics Institute

Miksi harjoittelu on tärkeää pk-yrityksen kyberturvassa?

Pk-yrityksissä kyberturva ei ole ensisijaisesti tekninen kysymys – se on liiketoiminnan jatkuvuus- ja johtamiskysymys.

- 1. Kyberuhkat iskevät arkeen – eivät IT-suunnitelmiin**
- 2. Ihmiset ovat suurin kyberriski – ja paras suoja**
- 3. Harjoittelu tekee ohjeista toimivia**
- 4. Kyberhäiriö = liiketoimintahäiriö (ti-to ketju)**
- 5. Harjoittelu tukee myös vaatimuksia ja kumppanuuksia**



ELI - European
Logistics Institute

Kyberharjoituksen esimerkkiskenaario

HARJOITUKSEN OSA	KUVAUS
Häiriön alku	Tietojenkalasteluviesti avataan ja järjestelmät hidastuvat.
Tilanteen eskaloituminen	Asiakkaat raportoivat epäilyistä, järjestelmät kaatuvat ja kiristysviesti ilmestyy.
Ensimmäisen tunnin toiminta	Johtovastuu, järjestelmien eristäminen ja ulkopuolisten kumppaneiden kontaktointi.
Viestintä	Henkilöstön ja asiakkaiden informointi oikea-aikaisesti.
Tavoite	Lisävahingon estäminen ja liiketoiminnan jatkuvuuden varmistaminen.



ELI - European
Logistics Institute

Kyberharjoituksen esimerkkiskenaario

HARJOITUKSEN OSA	KUVAUS
Mikä aiheuttaa korvausvastuun pk-yrityksessä? (esimerkkejä) Pk-yrityksen kannalta vastuu syntyy tyypillisesti, kun: • MFA puuttuu kriittisistä järjestelmistä • tietojärjestelmiä ei ole päivitetty • varmuuskopioita ei ole testattu • henkilöstöä ei ole koulutettu • kyberriskejä ei ole arvioitu lainkaan GDPR-käytäntö	varmistaminen.

Digitalisaation ja tietojärjestelmien haavoittuvuudet

Kyberuhkat logistiikassa: Digitalisaatio altistaa logistiikan kansainvälisille kyberuhille, jotka voivat häiritä toimitusketjuja ja aiheuttaa datamanipulaatiota.

GPS- ja AIS-manipulointi: GPS:n ja AIS:n manipulointi voi johtaa virheelliseen sijaintitietoon, vaarantaen erityisesti meriliikenteen turvallisuuden.

Häiriöt digitaalisissa prosesseissa: Digitalisoituneiden prosessien häiriöt voivat lamauttaa varastonhallinnan, reittisuunnittelun ja kuljetusten ohjauksen nopeasti.

Kyberturvan ja koulutuksen merkitys: Toimitusketjujen digitalisaatio vaatii vahvaa kyberturvaa, varajärjestelmiä ja henkilöstön koulutusta riskien hallitsemiseksi.



ELI - European
Logistics Institute

Kiitos!



ELI:n nettisivut
Vesa Vainio

www.xamk.fi/ELI/
[vesa.vainio\(at\)xamk.fi](mailto:vesa.vainio(at)xamk.fi)

