



Maanpuolustuskorkeakoulu

Luottamus teknologian mahdollistajana

Klaus Zaerens

Sotatieteiden päivät 2021



Puolustusvoimat

Försvarsmakten • The Finnish Defence Forces



Sisältö

- Laskennallisen luottamuksenhallinnan keskeisimmät ominaisuudet
- Luottamuksenhallinnan käyttökohteita
- Yleisiä haasteita ja ongelmia
- Tietojärjestelmissä huomioitavia näkökulmia
- Tulevia suuntauksia





Luottamukseenhallinnan määritelmiä

Luottamus

- is “a quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context”
(Grandison ja Sloman 2002).

Maine

- on käsitys, jonka toimija on aiemmillä teoillaan antanut pyrkimyksistään ja normeistaan
(Mui, Mohtashemi ja Halberstadt 2002).

Erityispiirteinä

- Kontekstisidonnaisuus
- Subjektiiivisuus
- Odotettu todennäköisyys
- Relevanttius





Laskennallisen luottamuksenhallinnan ominaisuuksia

Asymmetrisyys

- Jos A luottaa B :hen, B ei välttämättä luota A :han.

Kvantitatiivisuus

- Positiivisen tuloksen “todennäköisyys”
- Negatiivisen tuloksen riski
- Epäluottamuksen suuruus

Subjektiiivisuus

- Yksilölliset kokemukset tai mieltymykset voivat vaikuttaa kvantitatiiviseen arvoon

Transitiivisuus

- A luottaa B :hen ja B luottaa C :hen, jolloin A saattaa luottaa C :hen.

Domainsidonnaisuus

- Luottamus rajoittuu domainiin ja tiettyyn toimenpiteeseen tai toimenpiteiden luokkaan
- Reaalimaailmassa esiintyy harvoin absoluuttista luottamusta
- A voi luottaa B :hen joidenkin tehtävien suhteen, vaikka B ei olisi kompetentti, motivoitunut tai yleisesti ottaen luotettava

Roolipohjaisuus

- Käytännön toteutuksissa usein sidoksissa rooliin
- Luottamussuhde kahden joukon välillä ei välttämättä tarkoita luottamusta joukon alkioiden välillä





Luottamukseenhallinnan käyttökohteita





Yleisiä haasteita ja ongelmia

- Toimijoiden välinen luottamus ei välttämättä heijastu sisällölliseen luotettavuuteen
 - Tiedon oikeellisuus, ajantasaisuus ja oleellisuus.
 - Disinformaation vaikutukset ja käsittely.
- Tiedonvaihdon arvottaminen
 - Mitä on riittävä määrä tietoa jaettavaksi tai vaihdettavaksi?
- Absoluuttista luottamusta ei ole olemassa.
 - Jopa suljetussa luottamukseen perustuvassa systeemissä toiset toimijat ovat luotettavampia kuin toiset.
- Luottamuksen hallinta sinänsä ei ratkaise tiedon välityksen haasteita avoimessa verkossa
 - Tietovuodot
 - Tiedon kasautuminen kolmansille osapuolille
- Epäluottamuksen julkisuus
- Teknisiä haasteita
 - Suuret tietomäärät
 - Reaaliaikavaatimukset
 - Tiedon redundanttius
 - Tiedon siirtokapasiteetti
 - Väärä ja väärennetty tieto





Tietojärjestelmissä huomioitavia näkökulmia

- Yhä enemmän operatiivisia päätöksiä tehdään vastaanotetun tiedon perusteella
- Tiedon redundanttiudesta huolehtiminen
- Jaettavan tiedon arvon määrittäminen
- Kokonaisjärjestelmän haavoittuvuudet ja uhkien vaikutukset
- Vihamielisen tunkeutujan käsittelyn strategiat
- Tietolähteiden luotettavuus
- Luottamus vs yksityisyys
- Luottamuksenhallinnan erityistapaus: Luottamuksen kehä
 - Kaikki osapuolet luottavat toisiinsa
 - Yksittäisen toimijan mainearvo on merkityksetön
 - Yksittäinen mielipide korostuu, jos yhteistä mielipidettä ei ole muodostettu





Tulevia suuntauksia

- Tiedon jakamisen ja vaihdannan sovellukset
 - Tiedon monetisointi ja kaupankäynti
 - Oikeellisuus, relevanttius, ajantasaisuus
- Asioiden/Esineiden Internet (Internet of Things)
 - Verkottunut maailma, kaikkialla läsnä oleva ja äärimmäinen laaja-alaisuus
 - Päätelaitteiden määrän kasvu
 - Tiedon jakaminen ja tallettaminen
 - Luottamukseen perustuvat kokoonpanot
- Tietämyksen muodostaminen (Knowledge Management)
 - Ilmiöiden tunnistaminen
- Toimitusketjut- ja logistiikkajärjestelmät
 - Seuraavan sukupolven älykkäät sopimukset





Maanpuolustuskorkeakoulu

Kiitos!

Klaus.Zaerens@ecechiria.fi



Puolustusvoimat

Försvarsmakten • The Finnish Defence Forces

5.11.2021

9