Puolustusvaliokunnalle 5.4.2017

HYBRIDIVAIKUTTAMISESTA JA KYBERTURVALLISUUDESTA

KYBERTURVALLISUUDELLA tarkoitetaan erilaisia teknisiä ja hallinnollisia keinoja joilla digitaalisen infrastruktuurimme uhka hallitaan. Digitaalisella infrastruktuurilla tarkoitetaan tieto- ja viestintätekniikan, automaation ja niitä yhdistävien tietokoneohjelmistojen ja datan kokonaisuutta. Kyberturvallisuuden uhat voivat joko kohdistua digitaaliseen infrastruktuuriimme tai johtua siitä. **Tietoturvallisuus** on yksi keino saavuttaa riittävä kyberturvallisuuden taso.

Keskeiset erot kyberturvallisuuden ja tietoturvallisuuden välillä ovat:

1) Tietoturvallisuus on vanhastaan mielletty *tietojen* turvaamisena. Esidigitaalisella ajalla tiedot, tietojenkäsittely ja tietoa hyväksikäyttävät prosessit miellettiin erillisinä suojattavina kohteinaan. Viimeistään 2000-luvulla on kuitenkin alettu ymmärtää, että näkökulma on liian suppea. Tiedon rinnalla vähintään yhtä keskeisenä suojattavana kohteena ovat tietoja käsittelevät *järjestelmät*, eli tietoverkot, tietotekniikka, automaatiojärjestelmät ja tietokoneohjelmistot. **Kyberturvallisuuden käsitteistöllä pyritäänkin korostamaan sitä, että sekä järjestelmillä että niiden käsittelemillä tiedoilla on molemmilla välinearvo enenevässä määrin automatisoiduille yhteiskunnan perustoiminnoille ja että molempien suojaamiseen tulee panostaa.** Digitalisoidut prosessit eivät tuota ennustettavia (saati toivottavia!) tuloksia mikäli ne toteuttavat järjestelmät eivät ole hallittavissa ja mikäli niiden käsittelemät tiedot eivät säily luottamuksellisina, eheinä tai saavutettavissa. Kyberturvallisuus on näin ollen tietoturvallisuutta kattavampi termi kuvaamaan digitaalisen infrastruktuurin suojaamista ja siihen kohdistuvia uhkia.

2) Tietoturvallisuuden ja kyberturvallisuuden käsitteistö jakautuu myös suurvaltojen etupiirien mukaan. Noin kymmenen vuotta sitten Yhdysvallat liittolaisineen ryhtyi lanseeraamaan kyberturvallisuuden käsitteistöä tehdäkseen pesäeroa erityisesti Venäjän ja Kiinan pyrkimyksille käyttää "tietoturvallisuudesta huolehtimisen" menetelmiä sanan- ja mielipiteenvapauteen kohdistuville rajoituksille. Siinä missä Venäjän ja Kiinan edustama leiri pyrki laventamaan tietoturvallisuuden koskemaan sisältöjä, Yhdysvallat halusi tukeutua käsitteistöön joka nimenomaan viittaa tekniseen infrastruktuuriin ja jättää sisällöt arvottamatta. Venäjä ja Yhdysvallat jopa aktiivisesti pyrkivät synnyttämään yhteisen arvolatauksista vapaan käsitteistön[1], jotta keskeisistä konsepteista voitaisiin sopia valtioiden tasolla.

Huomionarvoista, että Suomen säädöskokoelmassa ei ole ainuttakaan[2] viittausta kyberturvallisuuteen, vaan yleensä käytetään ilmaisuja "tietoturvaloukkaus" ja "tietoturvasta huolehtiminen" myös silloin kun tarkoitetaan teknisen infrastruktuurin suojaamista, eli käytännössä kyberturvallisuutta.

Puolustusvoimien omaksumassa terminologiassa kyberturvallisuudella tarkoitetaan vastaavalla tavalla teknisen infrastruktuurin suojaamista. Kyberpuolustus puolestaan tarkoittaa sotilaallisen tehtävän (suojaaminen, tiedusteleminen tai vaikuttaminen) suorittamista ja suorituskykyjen käyttöä tieto- ja viestintäteknisen välineen avulla tai tietoverkoissa.

Puolustusvoimien omaksumassa filosofiassa kyberturvallisuuden kanssa likeinen käsite on operaatioturvallisuus: tapa toimia ja käyttää teknisiä välineitä tavalla joka ei vaaranna omasuojaa ja tehtävää. Yksilöllä tulee olla riittävä osaaminen ja sopivat välineet, jotta tämä voi suojata itseään, käyttämiään teknisiä alustoja ja tehtäväänsä teknisen infrastruktuurin kautta tapahtuvaa tiedustelua ja vaikuttamista vastaan. Puolustusvoimien omaksumaa filosofia on selkeä ja lähes sellaisenaan yleistettävissä mihin tahansa organisaatioon ja tehtävään, metsurista neuvottelevaan virkamieheen.

HYBRIDIVAIKUTTAMISELLA tai hybridioperaatioilla tarkoitetaan pyrkimystä vaikuttaa kohteeseen epätavanomaisia ja epäsuoria menetelmiä käyttäen, erityisesti digitaalista toimintaympäristöämme hyödyntäen. Hybridivaikuttamisella on leikkaavuuksia kyberturvallisuuteen. Hybridivaikuttamisen keinovalikoimaan kuuluu myös kyberturvallisuuden heikkouksien hyödyntäminen.

---

[1] https://www.files.ethz.ch/isn/178418/terminology2.pdf

[2] Poislukien VN:n päätös huoltovarmuuden tavoitteista vuodelta 2013.

Vakoilu on siirtynyt verkkoon ja siitä on tullut kybervakoilua. Nykyaikainen propaganda on lievimmillään informaatiovaikuttamista ja äärimmillään infosotaa - tietoa pimitetään, vuodetaan, luodaan, manipuloidaan ja sotketaan kulloisenkin poliittisen narratiivin tarpeisiin. Niin kutsuttu kineettinen vaikuttaminen tai selkokielisemmin sabotaasitoiminta on mahdollista toteuttaa myös kaukovaikutuksella, mielellään jopa kohteen omaa infrastruktuuria hyväksikäyttämällä. Mikäli tavoitteena on kohteen yhteiskuntajärjestyksen häirintä ja epävarmuuden synnyttäminen ilman avointa diplomaattista, sotilaallista tai taloudellista konfliktia, on hybridivaikuttaminen siihen oiva väline, koska toimeksiantaja ja toteuttaja voivat aina kiistää osallisuutensa.

Table 1. Summary table.

Feature	Conventional Conflict	Cyber Conflict
Primary means	Coercive, destructive	Non-coercive, transformative
Conflict structure	Centralized	Potentially ultra-decentralized
Form	Fixed	Mutable
Delimitation of war and peace	Present	Absent
Dynamics	Medium	High
Timeframe	Precise	Vague
Involvement of private interests	Medium	High
Participation of non-state actors	Medium	High
Capability for differentiation of targets	Medium	Low
Control of conflict means (in the case of massive strike)	High	Low
Intelligence, adversary's capabilities assessment	Efficient	Hampered
Military planning	Efficient	Hampered
Deterrence mechanisms	Present	Absent
Public perception of conflict	Direct	Mediated
Potential for deception regarding the conflict	Low	High
Existence of efficient social and legal mechanisms applicable to the conflict	Present	Absent
Infliction of direct social effect	Absent	Present

Kuva 1 Cyber Conflicts as a New Global Threat, Alexander Kosenkov, Information Society Research Center, Ukraine.

MITÄ AVOIMEMPI, demokraattisempi ja sopimusten noudattamiseen perustuvampi yhteiskunta on, sen alttiimpi se on hybridivaikuttamiselle. Valehteluun ja vääristelyyn kun ei voi vastata valehtelemalla ja vääristelemällä. Vaikuttamisoperaatioon ryhtyneen tahon ehdoilla tapahtuva dialogi ja vuoropuhelu eivät myöskään toimi ("Miksi olla vaikea kun pienellä vaivalla voi olla täysin mahdoton?").

Sen sijaan **hybridioperaatioihin ryhtyneen tahon toimintaan kohdistuva läpinäkyvyys on toteuttajalle ja toimeksiantajalle myrkkyä**. Mikäli operaatioita ei tunnisteta, ei niihin voida vastata. Mikäli hybridioperaatioiden vaikuttavuutta ei ymmärretä, ei niihin kenties edes nähdä tarvetta vastata. Mikäli operaatioiden "masinoitua luonnetta" ei tunnisteta, ei vastatoimia voida suunnata ja mitoittaa oikein.

HYBRIDIVAIKUTTAMISEN TUNNISTAMINEN edellyttää aiempaa tehokkaampaa dialogia teknisen infrastruktuurin tunnusmerkistöjä seuraavan tietoturvallisuusyhteisön sekä yhteiskunnallisia, taloudellisia ja poliittisia signaaleja seuraavan yhteisön välillä. Ei ole sattumaa, että monissa Euroopan maissa "kyberturvallisuuskeskuksiksi" kutsutut viranomaiset toimivat käytännössä poikkihallinnollisina fuusiokeskuksina, joissa tuotetaan kokonaisvaltaisesti tilannekuvaa yhteiskuntajärjestykseen digitaalisen toimintaympäristön kautta kohdistuvista uhista. Uhkien tekniset ilmenemismuodot on välttämättä liitettävä kontekstiin, jotta niiden merkitys osana kokonaisuutta valkenee, aiottu tavoite selviää ja tekijä paljastuu.

Erka Koivunen
Chief information Security Officer
F-Secure Corporation