HYBRIDIVAIKUTTAMISESTA JA KYBERTURVALLISUUDESTA

KYBERTURVALLISUUDELLA tarkoitetaan tieto- ja viestintätekniseen ja läpitunkevaan automatisointiin perustuvaan digitaaliseen infrastruktuuriimme kohdistuvia turvallisuusvaatimuksia ja -uhkia. **Tietoturvallisuus** on yksi keino saavuttaa riittävä kyberturvallisuuden taso. Huomionarvoista, että Suomen säädöskokoelmassa ei ole ainuttakaan[1] viittausta kyberturvallisuuteen, vaan yleensä käytetään ilmaisuja "tietoturvaloukkaus" ja "tietoturvasta huolehtiminen". Hybridivaikuttamisen keinovalikoimaan kuuluu myös kyberturvallisuuden heikkouksien hyödyntäminen.

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. Erityisesti 2000-luvulla on alettu ymmärtämään, että tiedon rinnalla vähintään yhtä keskeisenä suojattavana kohteena ovat tietoja käsittelevät *järjestelmät*, eli tietoverkot, tietotekniikka ja automaatiojärjestelmät. **Kyberturvallisuuden käsitteistöllä pyritään korostamaan sitä, että sekä järjestelmillä että niiden käsittelemillä tiedoilla on molemmilla välinearvo yhteiskunnan perustoiminnoille ja että molempien suojaamiseen tulee panostaa.** Digitalisoidut prosessit tuota enää ennustettavia (saati toivottavia!) tuloksia mikäli ne toteuttavat järjestelmät eivät ole hallittavissa ja mikäli niiden käsittelemät tiedot eivät säily luottamuksellisina, eheinä tai saavutettavissa.

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[2], jotta keskeisistä konsepteista voitaisiin sopia valtioiden tasolla.



HYBRIDIVAIKUTTAMISELLA tai hybridioperaatioilla tarkoitetaan pyrkimystä vaikuttaa kohteeseen epätavanomaisia ja epäsuoria menetelmiä käyttäen, erityisesti digitaalista toimintaympäristöämme hyödyntäen. Hybridivaikuttamisella on leikkaavuuksia kyberturvallisuuteen. 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.



[1] Poislukien VN:n päätös huoltovarmuuden tavoitteista vuodelta 2013.
[2] https://www.files.ethz.ch/isn/178418/terminology2.pdf

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
Cyber Security Advisor
F-Secure Corporation