Kybersodan aika on alkamassa

Vuosina 1946-1958 Pohjois-Tyynenmeren Bikini-atollia käytettiin testauskenttänä 23 uudelle ydinaseelle, jotka räjäytettiin eri kohdissa sen päällä, yläpuolella tai alla. Testien tarkoitus oli ensisijaisesti ymmärtää ja monissa tapauksissa esitellä, kuinka nämä uudet aseet todella toimivat ja mihin ne pystyivät.

Ydinkokeiden aikakausi saattaa olla ohi, mutta kybersodan aika on vasta alkamassa. Venäjälle sota Ukrainan kanssa on todennäköisesti toiminut elävänä testausalueena seuraavan sukupolven kyberaseille.

Toisin kuin perinteiset hyökkäykset, kyberhyökkäyksiä voi olla vaikea määrittää tarkasti. On vaikea todistaa, kuka hyökkäyksen takana on. Monissa tapauksissa kyberhyökkäyksiä voidaan käynnistää haltuunottettujen, eli hakkeroitujen tietokoneiden ja tietoverkoissa olevien laitteiden kautta.

Huonosti suojattu tietokone tai verkkolaite voidaan ottaa hyökkääjän haltuun käyttäjän tietämättä ja käyttää hyökkäysketjun käynnistämiseen. Vuonna 2016 tuhansia kodin turvakameroita otettiin haltuun ja niitä käytettiin häiritsemään Twitterin, Amazonin, Spotifyn, Netflixin ja monien muiden toimintoja.

On vahvaa näyttöä siitä, että venäläiset hakkerit ovat toteuttaneet kyberhyökkäysten sarjan Ukrainassa. Vuonna 2015 Krimin valtauksen jälkeen hakkerit onnistuivat katkaisemaan sähkön noin 230 000 asiakkaalta Länsi-Ukrainassa. Seuraavana vuonna hyökkäys kohdistui valtion virastoihin ja pankkijärjestelmään.

Tänä vuonna, tuntia ennen venäläisten joukkojen hyökkäystä, Ukrainaan törmäsi ennennäkemätön haittaohjelma, joka oli suunniteltu pyyhkimään tietoja Ukrainan hallinnon eri järjestelmistä.

Ukrainan hallituksen mukaan hyökkäys oli täysin eri tasolla kuin aikaisemmat hyökkäykset.

Ukraina on houkutteleva kohde kybersotavalmiuksien testaamiseen. Maassa on samanlainen infrastruktuuri kuin Länsi-Euroopassa ja Pohjois-Amerikassa. Ukrainalla on kuitenkin rajallisemmat resurssit vastahyökkäykseen, vaikka Yhdysvallat ja EU ovat molemmat tukeneet Ukrainaa kyberpuolustuksensa vahvistamista.

Vaikka Venäjä on ilmeinen epäilty, on mahdollista, että muutkin maat, kuten Iran, Pohjois-Korea tai Kiina, ovat testanneet omia kyberaseitaan Ukrainassa.

Laajamittainen kyberkahakka voi tulla globaaliksi niin sanotun heijastusvaikutuksen vuoksi. Vuonna 2017 epäilty venäläinen hyökkäys jossa NotPetya-niminen haittaohjelma häiritsi Ukrainan lentokenttiä, rautateitä ja pankkeja.

NotPetya ei kuitenkaan jäänyt Ukrainaan. Se levisi nopeasti ympäri maailmaa tartuttaen ja osin sulkien useita monikansallisia yrityksiä, mukaan lukien maailmanlaajuisen laivayhtiö Maerskin ja lääkejätti Merckin.

Useimmat kyberhyökkäykset eivät ole vielä olleet niin tuhoisia kuin ne olisivat voineet olla. Hyökkäykset ovat olleet todennäköisesti vain kyberaseiden testejä. Täysimittainen kyberhyökkäys, huomioon ottaen kriittisten infrastruktuurialojen, kuten sähkön ja viestinnän keskinäisen riippuvuuden, todennäköisesti kaataisi useita sektoreita samanaikaisesti.

Hyökkäyksen ensisijainen tavoite olisi tuottaa pitkäkestoisia fyysisiä, koko infrastruktuuriin kohdistuvia vahinkoja.

Länsimaissa on huomioitava erityisesti, että kyberhyökkäykset tuskin rajoittuvat pelkästään Ukrainaan. Hallitusten ja yritysten tulisi seurata tarkasti, mitä Ukrainassa tapahtuu, koska kybersota voi ja on jo levinnyt nopeasti rajojen yli.

Ismo Turve

Kirjoittaja on kyberturvallisuus orientoitunut heinolalainen Tietojenkäsittelyn lehtori Hämeen ammattikorkeakoulusta.