Terroristide ja Interneti suhtest

24 aastat tagasi - 08.11.2001 Autor: AM

Autor: **Jani Heikkilä**

Ühest vaatepunktist lähtudes on Internet suur avalik raamatukogu, millel on sadu miljoneid kasutajaid: ainüksi WWW-s on hetkel üle miljardi lehekülje. Igal inimesel või organisatsioonil on võimalik leida veebist sellist informatsiooni, millest oleks terroristlike kuritegude planeerimisel palju kasu. Näiteks: aadresse, seadusi, analüüse ja vestluseid, mis puudutavad oletatava organisatsiooni oletatavat missiooni.

Internetist on võimalik leida avaliku elu tegelaste nimesid, numbreid ja e-posti aadresse ning saata otse nendele propagandat või mida tahes.

Interneti abil on edukalt õnnestunud rikkuda riikide poolt kehtestatud tsensuuri; sellest on loomulikult palju abi terroristidele. Aga Internet ei ole kõigest hoolimata täielikult kontrollimatu. "Reporters Sans Frontiersi" järgi on maailmas 45 riiki, mis püüavad kontrollida oma kodanike kokkupuuteid ülemaailmse võrguga. Kontrolli olemus on lihtne: kodanikele pakutakse ainult ühte ISP-d (Interneti teenuse pakkujat), mis on riigi kontrolli all. Nii on juba väga lihtne filteerida lehekülgi, mida tohib vaadata ja mida mitte.

Kuidas siis kasutavad terroristid Internetti?

Tegelikult on terroristidel tohutult palju võimalusi veebi kasutamiseks, kuid neid võiks jaotada kolme peamisse gruppi: propaganda, kommunikatsioon ja küberterrorism.

Internet pakub erinevaid viise oma propaganda levitamiseks. Gruppidel on võimalus teha isiklikud koduleheküljed ja nende kaudu näiteks raha koguda, väljendada oma poliitilisi vaatepunkte ja leida loomulikult ka uusi liikmeid. Mitmel organisatsioonil, mida erinevate riikide ametnikud nimetavad terroristlikeks, on olemas omad veebilehed. Kuna suuremas osas maailmas on sõnavabadus ja neil saitidel ei räägita otseselt kuritegudest, siis ei luba kehtivad seadused neid kinni panna. Seoses septembrikuiste sündmustega USA-s on teada muidugi ka paar erandit, mil suleti nii mõnigi kahtlustäratav sait.

Lisaks oma ideede propageerimisele pakub Internet ka rohkelt võimalusi valeinfo levitamiseks vaenlaste kohta. Informatsiooni levitamiseks Internet on odavam, kui

traditsionaalsete massimeedia vahendite kasutamine. Veebilehtede omamine ja tegemine on ju suurel määral tasuta ja samuti ei tekita e-maili kasutamine ning vestlusgruppides osalemine mingeid erilisi väljaminekuid.

Tänu Internetile on organisatsioonidel lihtne jaotuda väiksemateks gruppideks. Neil on võimalik levitada informatsiooni elektronposti teel, kodeerida ja krüpteerida oma sõnumeid või paigutada need otse veebilehele. Telefone ega fakse pole enam vaja, samuti kaovad geograafia ja ajaga seotud probleemid.

Üle kogu maailma on küllalt punkte, kus saab Internetti kasutada vabalt valitud ajal. Loomulikult vajab see korralikku ühendust ja seda on mõnes kohas (õnneks) raske saada.

Võrgus on võimalik teha ka otseseid pahateguseid, mitte ainult ühendust pidada või infot levitada. Üks lihtsamatest viisidest on kasutada näiteks kirjapomme, millega häiritakse kirjade liiklust ja proovitakse servereid üle koormata ning muuta igapäevane töö võimatuks. Ilmselt oli esimene kirjapommidega seotud terroriakt aastal 1998. Siis saatsid Sri Lanka Tamili sissid kohalikesse saatkondadesse kahe nädala jooksul iga päev üle 800 e-kirja, kus õeldi "We are the Internet Black Tigers of Tamil and we are doing this to disrupt your communications". ("Meie oleme Tamili Interneti Mustad Tiigrid ja teeme seda selleks, et segada teie ühendust"). Sellega pälvisid nad väga suurel hulgal avalikkuse tähelepanu ja seega oli nende tegu hästi õnnestunud. Peale Tamili terroristide on teisedki rühmitused sarnaseid akte korraldanud. Ajakirjandus võtab alati kinni sellest, mis juhtub arvutite ja Internetiga, sest teema on võrdlemisi uus ja huvitav.

Kuidas häkkerid tegutsevad?

Kokkuvõtvalt võib öelda, et nende peamiseks leivanumbriks on arvutivõrkude töö segamine, valeinfo tekitamine ja lekitamine, teabe varastamine ja loomulikult ka viiruste valmistamine ning laiali saatmine.
Kujutage ette, milliseid tagajärgi võib tuua info varastamine näiteks pangast või riigiametitest; sama olukord on siis, kui valedesse kätesse satuvad ehitiste plaanid või ülisalajased dokumendid. Sel põhjusel sulges ka Pentagon oma virtuaalse kodu kohe pärast rünnakuid ega ole seda siiani avanud.
Eelpool mainitu ei ole aga ainult terroristide pärusmaa, samu vahendeid kasutavad ka mitmed paramilitaarsed grupid ja paljud vähemused.
Kõikvõimalikud aktivistid, kellele meeldib demonstratsioone korraldada, (tuletage meelde G8 tippkohtumisel toimunud veriseid protestiaktsioone) saavad omavahel väga lihtsate vahenditega suhelda ning muutuvad niimoodi eriti tugevaks. See on

ka põhjus, miks nad on nii hästi organiseeritud. Kui veebiteel suhtlemine erilisi finantsilisi kulutusi ei nõua (sageli teevad osavamad protestimeelsed kodanikud koduka ise kiiruga valmis), siis muu tegevus on juba palju kulukam. Sellegi probleemi lahendamisel tuleb appi Internet: mitmetel kodulehekülgedel saavad krediitkaardiga külastajad endale meelepärast rühmitust rahaliselt toetada. See ei võta ei aega ega pingutust.

LINGID:

www.state.gov U.S. Department of State, USA Riigidepartemang
www.adl.org Anti-Defamation League, avaliku laimu vastane lehekülg
www.Terrorism.com The Terrorism Research Center, Terrorismi uuringukeskus
www.teror.gen.tr/english/organisations Terroriorganisatsioonide loetelu
www.ict.org.il The International Policy Institute for Counter - Terrorism
killeenroos.com/link/terror.htm

- Uudised
- Turvalisus