Maanpuolustuskorkeakoulu
Johtamisen ja
sotilaspedagogiikan laitos
00860 Helsinki
Suomi Finland

Puh: +358 (0)299 530411
www.mpkk.fi

ISBN 978-951-25-2088-6
ISBN PDF 978-951-25-2088-6
ISSN 1798-0399

Saara Jantunen
'Kiinalaiset kybersoturit'
Julkaisusarja 1, Nro 4/2010

UUSIEN UHKAKUVIEN LUOMINEN: TAPAUS 'KIINALAISET KYBERSOTURIT'

Lingvistinen uhka-analyysi kyberdiskurssista

Saara Jantunen

Maanpuolustuskorkeakoulu
Johtamisen ja sotilaspedagogiikan laitos
Julkaisusarja 1: Tutkimuksia Nro 4

Maanpuolustuskorkeakoulun Johtamisen ja sotilaspedagogiikan laitos

UUSIEN UHKAKUVIEN LUOMINEN: TAPAUS ’KIINALAISET KYBERSOTURIT’ – Lingvistinen uhka-analyysi kyberdiskurssista

Saara Jantunen

Maanpuolustuskorkeakoulun Johtamisen ja sotilaspedagogiikan laitoksen
Julkaisusarja 1 – Tutkimuksia 4/2010

Toimittanut: Torsti Sirén
Kannen kuva: Jussi Simpanen

ISBN 978-951-25-2087-9
ISBN PDF 978-951-25-2088-6
ISSN 1798-0399
Edita Prima Oy
Helsinki 2010

SISÄLLYS

ABSTRACT

Creating Modern Threat Scenarios: A Case Study on the Narrative of Chinese Cyber-Warriors

Since his inauguration, President Barack Obama has emphasized the need for a new cybersecurity policy, pledging to make it a "national security priority". This is a significant change in security discourse after an eight-year war on terror – a term Obama announced to be no longer in use. After several white papers, reports and the release of the so-called *60-day Cybersecurity Review*, Obama announced the creation of a "cyber czar" position and a new military cyber command to coordinate American cyber defence and warfare. China, as an alleged cyber rival, has played an important role in the discourse that introduced the need for the new office and the proposals for changes in legislation.

Research conducted before this study suggest the dominance of state-centric enemy descriptions paused briefly after 9/11, but returned soon into threat discourse. The focus on China's cyber activities fits this trend. The aim of this study is to analyze the type of modern threat scenarios through a linguistic case study on the reporting on Chinese hackers. The methodology of this threat analysis is based on the systemic functional language theory, and realizes as an analysis of action and being descriptions (verbs) used by the American authorities. The main sources of data include the *Cybersecurity Act 2009*, *Securing Cyberspace for the 44th Presidency*, and *2008 Report to Congress of the U.S. - China Economic and Security Review Commission.*

Contrary to the prevailing and popularized terrorism discourse, the results show the comeback of Cold War rhetoric as well as the establishment of a state-centric threat perception in cyber discourse. Cyber adversaries are referred to with descriptions of capacity, technological superiority and untrustworthiness, whereas the ‘self’ is described as vulnerable and weak. The threat of cyber attacks is compared to physical attacks on critical military and civilian infrastructure. The authorities and the media form a cycle, in which both sides quote each other and foster each other’s distrust and rhetoric. The white papers present China's cyber army as an existential threat. This leads to cyber discourse turning into a school-book example of a securitization process. The need for security demands action descriptions, which makes new rules and regulations acceptable. Cyber discourse has motives and agendas that are separate from real security discourse: the arms race of the 21st century is about unmanned war.

Keywords: Systemic Functional Linguistics, threat analysis, cyber warfare, China, securitization

1. JOHDANTO

Kyberuhkia on nostettu voimakkaasti pinnalle sekä julkisessa mediassa että USA:n hallinnossa. Vuosina 2007 ja 2008 Kiinaa syytettiin aggressiivisesti hakkeroinnista ja vakoilusta, ja vuoden 2008 lopussa U.S.-China Economic and Security Review Commission esitti kongressille erittäin jyrkkälinjaisen raportin Kiinan kybertoiminnasta. Pian virkaanastumisensa jälkeen Barack Obama nimitti ”kybertsaarin” johtamaan niin sanottua ’kuudenkymmenen päivän kyberturvallisuuskatsausta’. Tämä tutkimus ei ollut ainoa Obaman tilaama raportti, vaan raportteja on esitelty kevään mittaan useita. Maaliskuussa Pentagon julkaisi vuotuisen *Military Power of the People's Republic of China* -raporttinsa, joka esittää suhteellisen varovaisia arvioita Kiinan kybersodankäyntikapasiteetista, mutta toteaa kuitenkin sen olevan hyvä. Samaan aikaan kanadalainen tutkimusryhmä julkaisi *Ghostnet*-raporttinsa, ja Iso-Britanniassa otsikoihin nousi *Snooping Dragon*-raportti. Obama ilmoitti poistavansa käytöstä termin ’terrorisminvastainen sota’, ja viikkoa myöhemmin Pentagon julkaisi tiedotteen, joka kertoi puolustusministeriön käyttäneen viimeisen kuuden kuukauden aikana 100 miljoonaa dollaria kyberpuolustukseen. Huhtikuussa kongressille tehtiin lakialoite, joka oikeuttaisi Valkoisen Talon määrittelemään hätätilan ja sulkemaan sekä julkisen että yksityisen sektorin verkkoliikenteen

Kiinaa on tasaisin väliajoin syytetty verkkovakoilusta läpi 2000-luvun. Miksi Kiinaa syytetään hakkeritoiminnasta, ja miksi juuri nyt? USA:n viimeaikainen retoriikka on keskittynyt terrorismiin, ja keskeneräisiä sotia on kaksi. Silti hakkeriuutiset ja kyberpuolustus saavat mediassa ja valtion toimielimissä osakseen suurta huomiota.

Tämän tutkimuksen tarkoituksena on lähestyä hakkerointitapauksiin liittyvää turvallisuusdiskurssia ja määrittää tämän diskurssin kielelliset valinnat, jotta ne voi asettaa systemaattisesti analysoitavaksi lingvistiseen viitekehykseen. Tavoitteena on määrittää kyberretoriikan nykyisen turvallisuuskäsityksen rakennetta ja kielellisiä piirteitä, jotta tarkka, käsitteellistävä lingvistinen analyysi voisi tukea laajempaa, poliittisia teemoja tarkastelevaa tutkimusta.

Tutkimuksen toinen luku käsittelee kyberdiskurssin historiaa ulko- ja turvallisuuspoliittisessa kontekstissa, ja nostaa esiin turvallistamistutkimuksen. Kolmas luku pohtii tietoverkkosodankäyntiä informaatio-operaationa ja vallankäyttönä, sekä sen asemaa yhteiskunnassa. Neljännessä ja viidennessä luvussa jäsennetään lingvistinen tutkimusviitekehys ja metodiikka, jota voidaan hyödyntää uhka-analyysissa uhkakuvien kielellisessä määrittelyssä. Paljon käytettyä, ns. Kööpenhaminan koulun metodia täydennetään soveltumaan kielitieteelliseen tutkimukseen. Viides ja viimeinen luku pohtii

kyberdiskurssin sisältämien uhkakuvien merkitystä turvallisuuspolitiikassa.

2. KÄÄNTEITÄ 2000-LUVUN UHKAKUVA-DISKURSSISSA

2.1. Valtiot, terroristit, vai molemmat?

Tietoverkkosodankäyniin liittyvää uhkadiskurssia leimaa ristiriitaisuus, muuttuvat uhkakuvat sekä strategiattomat ratkaisumallit, kirjoittaa Ralf Bendrath (2004), jonka tutkimus toimii erinomaisena johdantona kyberdiskurssin historiaan. Samaan aikaan kun USA:n viranomaiset julkaisevat raporttejaan Kiinan tietoverkkosodankäynnin kapasiteetista ja verkkohyökkäyksistä, Kiina syyttää USA:ta ”kylmän sodan mentaliteetista” ja tuomitsee verkkohyökkäykset moraalittomina (Wall Street Journal, 8.4.2009; China Daily 21.5.2009).

Vuonna 1990 National Academy of Sciences julkaisi raportin, jonka ensimmäiset lauseet olivat seuraavat (Bendrath, 2004):

> *“We are at risk. Increasingly, America depends on computers… Tomorrow’s terrorists may be able to do more damage with a keyboard than with a bomb.”*

Keväällä 2009 julkaistun lakialoitteen (Cybersecurity Act 2009) avauslause kuulostaakin tyylillisesti hyvin tutulta:

> *“The congress finds the following: America’s failure to protect cyberspace is one of the most urgent national security problems facing the country.”*

Eikä siinä vielä kaikki. Tietoverkkohyökkäystä verrataan suoraan syyskuun terrori-iskuun:

> *“According to the National Journal, Mike McConnell, the former Director of National Intelligence, told President Bush in May 2007 that if the 9/11 attackers had chosen computers instead of air planes as their weapons and had waged a massive assault on a U.S. bank, the economic consequences would have been ‘‘an order of magnitude greater’’ than those cased by the physical attack on the World Trade Center.”*

Näiden julkilausumien välillä on lähes 20 vuotta, mutta retorisesti ne ovat lähes identtisiä. Niiden yhteinen viesti on se, että teknologiariippuvuus ja tietoverkot ovat suurimpia Amerikkaa (ja ihmiskuntaa) uhkaavista

tekijöistä. Niiden rinnalla kalpenee jopa yli 3 000 ihmishenkeä vaatinut isku World Trade Centeriin.

Kun tietoverkot vuonna 1990 määriteltiin uusiksi uhkakuviksi, oli Neuvostoliitto juuri kaatunut, kylmä sota saapumassa päätökseensä, ja USA:lla tuli tarve uudelle ulkopuoliselle uhalle (Bendrath, 2004). Termi ”elektroninen Pearl Harbor” kuvastaa internetin siirtymistä sodankäynnin piiriin. Nykyversio siitä lienee ”Cyber Katrina” (Cybersecurity Act 2009), jolla tietoverkkouhkat rinnastetaan syyskuun terrori-iskujen lisäksi äärimmäiseen luonnonkatastrofiin, jota vastaan kansakunta on täysin avuton. Bendrathin mukaan kyberdiskurssi muuttui dramaattisesti George W. Bushin kaudella, jolloin esiin nostettiin valtiolliset uhat, eritoten nopeasti teknologian saralla kehittyvä Kiina. Ennen tätä suurimpana uhkana oli pidetty terrori-iskuja.

Terroristeja ei täysin unohdettu, mutta Bushin retoriikkaan liitettiin käsite ”roistovaltiot”, jotka pian laskettiin myös kyberuhkien joukkoon. Bendrath toteaakin, että sanalla ’cyber’ on suurempi merkitys retoriikassa ja salaisissa agendoissa, kuin todellisina vihollisina tai uhkina (2004). Kiinaa ei laskettu roistovaltioksi, vaan sitä pidettiin strategisena kilpailijana. Jo vuonna 2001 USA:n todettiin olevan informaatioteknologisessa varustelukilvassa (Bendrath, 2004). Kiinan syytös amerikkalaisten kylmän sodan mentaliteetista ei siis liene tuulesta temmattu.

Kiinan rooli kyberuhkakeskustelussa on jatkuvasti liittynyt maan väitettyyn haluun ja aikomukseen käyttää kyberhyökkäyksiä osana epäsymmetristä sodankäyntiä. Keväällä 2001 alkanut uhkakuvien määrittely laajeni kesällä 2001 koko NATOa koskevaksi, kun Rumsfeld ilmoitti puolustusyhteisön olevan vaarassa, ja syyskuuhun 2001 mennessä hallitus oli määritellyt uuden, valtiokeskeisen kyberuhkan (Bendrath, 2004).

Syyskuun terrori-iskut käänsivät uhkadiskurssin takaisin terrorismikeskeisyyteen. Välittömästi iskujen jälkeen *USA Today* lainasi ”entistä Pentagonin virkamiestä” ja varoitti mahdollisista kyberterrori-iskuista, ja kuun lopulla Bush perusti Office of Cyberdefencen (Bendrath, 2004). Terrori-iskun aiheuttamaa paniikkia käytettiin siis tehokkaasti hyödyksi kyberuhkakuvien vahvistamisessa.

Bendrathin mukaan media, virkamiehet ja tiedustelupalvelut luovat noidankehän, jossa kaikki lietsovat toistensa kauhuskenaarioita (2004). Sama ilmiö on huomattavissa nyt vuonna 2009. Raflaavan retoriset toteamukset pääsevät joskus myös lakialoitteiseen asti, kuten paljon lainatun *Securing Cyberspace for the 44th Presidency* -raportin kohdalla:

> *"America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009."*
> (Securing Cyberspace for the 44th Presidency)

Lakialoitteen ensimmäisen lauseen mukaan uhattuna ei ole pelkästään uusi hallitus, vaan koko maa. Lause on lähes suora lainaus virkamiesraportista:

> *"America's failure to protect cyberspace is one of the most urgent national security problems facing the country."*
> (Cybersecurity Act 2009)

Viranomaiset vievät spekulaation ennusteiden kautta faktoiksi. Ensin kerrotaan Kiinan kehityksestä verkkosodankäynnissä ja aikeista käydä verkkosotaa USA:ta vastaan:

> *"China's government is devoting a great deal of attention and resources to developing outer space and cyber space capabilities. China's military strategists view the U.S.' dependence on space assets and information technology as its ''soft ribs and strategic weaknesses.'' These investments by China's military potentially could provide it with an asymmetric capability enabling it to prevail in a conflict with U.S. forces."* (2008 Report to Congress of the U.S. – China Economic and Security Review Commission)

> *"Colonel McAlum said that China currently has the intent and capability to conduct cyber operations anywhere in the world at any time. China has an active cyber espionage program. Since China's current cyber operations capability is so advanced, it can engage in forms of cyber warfare so sophisticated that the United States may be unable to counteract or even detect the efforts."* (2008 Report to Congress of the U.S. – China Economic and Security Review Commission)

Mukaan voidaan liittää konkreettisia uhkakuvia, kuten seuraavissa lainauksissa raporteista:

> *"Internet-connected networks operate the national electric grid and distribution systems for fuel. […] A successful attack on these Internet-connected networks could paralyze the United States."* (2008 Report to Congress of the U.S. – China Economic and Security Review Commission)

> *"China is aggressively pursuing cyber warfare capabilities that may provide it with an asymmetric advantage against the United States."* (2008 Report to Congress of the U.S. – China Economic and Security Review Commission)

Uhkaa perustellaan kertomalla mitä Kiinan virkamiehet ja hallitus ajattelevat, sekä kertomalla miksi hyökkäys on täysin odotettavissa:

> *"Many Chinese authors believe the United States already is carrying out offensive cyber espionage and exploitation against China. China therefore must protect its own assets first in order to preserve the capability to go on the offensive."* (2008 Report to Congress of the U.S. – China Economic and Security Review Commission)

> *"Many PLA strategists believe there is a first mover advantage in both conventional and cyber operations against the United States. Therefore, in order to succeed, they should strike first."* (2008 Report to Congress of the U.S. – China Economic and Security Review Commission)

Seuraava, muutamaa kuukautta myöhemmin julkaistu raportti toteaa asian nykytilan, johon siihenkin voidaan liittää uhka ja pelote. Raportti on sama jota *Cybersecurity Act of 2009* lainasi:

> *"In cyberspace, the war has begun."* (Securing Cyberspace for the 44th Presidency)

> *"It is a battle we are losing."* (Securing Cyberspace for the 44th Presidency)

Bendraft (2004) toteaa, että tavallisen kansalaisen ei ole mahdollista tietää, onko kybersota todellisuutta vai ei, toisin kuin kylmän sodan aikana ydinaseiden kohdalla. Kuinka sitten suhtautua seuraavanlaiseen uutisointiin, joka lienee kuin vastaus hallituksen rukouksiin?

> *"Chinese military hackers have prepared a detailed plan to disable America's aircraft battle carrier fleet with a devastating cyber attack, according to a Pentagon report obtained by The Times."* (*The Times*, 8.9.2007)

> *"Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials."*(Wall Street Journal, 8.4.2009)

> *"Computer spies have broken into the Pentagon's $300 billion Joint StrikeFighter project -- the Defense Department's costliest weapons program ever -- according to current and former government officials familiar with the attacks."* (Wall Street Journal, 21.4.2009)

Tosiasia on, että kansalaisella ei ole mahdollisuutta arvioida kyberuhkien todellista laatua, tai tietää ovatko tässä kuvatut hyökkäykset todellisuutta, ja jos ovat, niin ovatko julkisuudessa kerrotut tekijät todella niistä vastuussa.

Tutkimuksessaan Bendrath (2004) on huomannut yllä kuvatun diskurssin kaltaisen ilmiön lehtien otsikoissa. *"Kun yleisöön on istutettu vahva usko vaanivasta kyberterrori-iskusta, seuraava askel on väittää, että se on jo tapahtunut."* On selvää, että terrorismikortti on julkisen mielipiteen ja suhtautumisen kannalta oleellinen sekä valtiollisia vihollisia korostavaa retoriikkaa tehokkaampaa syyskuun terrori-iskujen jälkeen. Kuitenkin jo kesällä 2002 valtiot palasivat hallituksen uhkakuvien keskiöön sillä perusteella, että vain valtiot ovat kyllin voimakkaita ollakseen vakavasti otettava kyberuhka (Bendrath, 2004).

Yllä kuvattu diskurssi on informaatio-operaatioiden, turvallistamisprosessin ja juonitetun, 'sotaan' valmistavan diskurssin malliesimerkki. Se legitimoi tehokkaasti hallituksen sotilaalliset ja taloudelliset toimet, ja toimii perusteena turvallistamisprosessille, jonka seurauksena valtiovalta ulottaa kontrollinsa myös yksityiselle IT-sektorille.

2.2. "Hallitus kantaa päävastuun"

> *"The United State must treat cybersecurity as one of the most important national security challenges it faces. Cybersecurity can no longer be relegated to information technology offices and chief information officers. Nor is it primarily a problem for homeland security and counterterrorism. And it is completely inadequate to defer national security to the private sector and the market. This is a strategic issue on par with weapons of mass destruction and global jihad, where the federal government bears primary responsibility."* (Securing Cyberspace for the 44th presidency)

Lakialoite *Cybersecurity Act 2009* esittää yksityisen ja valtion IT-sektorin yhteistyötä sekä yksityiselle sektorille yltävää valtiollista kontrollia. Lakialoitteen huomattavin ehdotus on kyberturvallisuuden valtiollistaminen, mikä merkitsisi sitä, että presidentin alaisuudessa toimiva

kyberturvallisuusneuvonantaja saisi oikeuden turvallisuusstandardien määrittämiselle ja tarvittaessa tietoturvahätätilan julistamiselle. Tällöin hän saisi määrätä sekä julkisen sektorin että kriittisen infrastruktuurin internet-liikenteen katkaistavaksi. Kriittiseen infrastruktuuriin luetaan mm. yksityissektoriin lukeutuvat pankit, energialaitokset sekä teleoperaattorit. Hallituksen viesti on se, että kyberuhkien torjunnan täytyy tapahtua koordinoidusti hallituksen kautta, ja että kyberuhat ovat hallituksen vastuualuetta.

Niin sanotun ”kybertsaarin” nimittämistä esittävät useat viranomaistahot, mm. INSA, sekä raporteista *Securing Cyberspace for the 44th Presidency* sekä Presidentti Obaman tilaama ja paljon huomiota saanut *60-day Cybersecurity Review*. Toukokuussa 2009 Presidentti Obama ilmoitti päätöksestään luoda kyseinen virka Valkoisen Talon alaisuuteen (Wall Street Journal, 29.5.2009).

Näillä keinoilla internet- ja tietoverkkoturvallisuus turvallistetaan ja siirretään pois poliittisesta päätöksenteosta suljetun sisäpiirin vastuualueeksi. Siitä tulee paniikkipolitiikkaa, josta ei keskustella avoimesti, tai johon ei voida vaikuttaa demokratian keinoin: turvallisuuden varjolla politiikkaa voidaan viedä pois sovittujen politiikan sääntöjen piiristä ja siitä voidaan tehdä joko erityispolitiikkaa, tai politiikkaa ”harvoille ja valituille” (Buzan, Waever & de Wilde, 1998). Käsite ’kansallinen turvallisuus’ on korvaamassa vanhaa tuttua ’kansallista intressiä’, ja olemme siirtyneet pysyvän poikkeustilan politiikkaan, ja poikkeustilasta päättäminen määrittelee vallankäyttäjän (Pulkkinen, 2004). Tämä on täydellinen kuvaus *Cybersecurity Act 2009*:n etenemisestä ja toteutumisesta.

Oleellista turvallistamisprosessissa on eksistentiaalinen uhka, joka vaatii kaikkien mahdollisten keinojen käyttöönottoa. Sotilassektorilla tämä uhka on yleensä toinen valtio (Buzan, Waever & de Wilde, 1998). Tältä kannalta katsottuna USA:n viranomaisten Kiina-retoriikka vaikuttaa hyvin loogiselta. Mikäli internet voidaan turvallistaa, valtion kontrolli- ja valvontamahdollisuudet paranevat. Buzan, Waever & de Wilde (1998: 25) toteavat, että kun turvallistaja onnistuu muuttamaan häntä normaalisti sitovia käytänteitä ja sääntöjä turvallisuuteen vedoten, ja kun yleisö hyväksyy nämä muutokset, todistamme onnistunutta turvallistamista. Turvallistaminen vaatii siis eksistentialistisilta uhilta legitiimiyttä, jotta ne ovat tarpeeksi painavia syitä perinteiden ja sääntöjen muuttamiselle. Kyse on siis myös yleisön arvomaailmaan vaikuttamisesta. Kyse on pohjimmiltaan samasta asiasta kuin vuoden 2003 Irak-retoriikka, jossa perusteena hyökkäykselle pidettiin joukkotuhoaseita (eksistentiaalinen uhka) sekä uusien terrori-iskujen mahdollisuutta. Viholliselle luotiin

identiteetti (moraaliton, brutaali, sortava), jonka avulla sota ”brändättiin” vapautusoperaatioksi.

Millä tavoin Kiinan toiminta tullaan brändäämään? Tullaanko Kiinasta puhumaan roistovaltiona, terroristimaana, vai siirrymmekö takaisin kylmän sodan retoriikkaan (Huhtinen & Rantapelkonen, 2007:92)? Buzan, Waever & de Wilde (1998: 27) toteavat, että turvallistamisdiskurssi ei välttämättä vaadi sanan ”turvallisuus” käyttämistä. Kun valtiot kaikesta terrorismi-retoriikasta huolimatta ovat uhkadiskurssin keskiössä, on tutkittava sitä, millä tavalla valtioiden aiheuttamaa uhkaa kielessä kuvaillaan. Tähän aiheeseen syvennytään 3. ja 4. luvun teoriassa ja kielianalyysissa.

2.3. ”Tuhannet ihmiset kuolevat”

Kynnyskysymykseksi kyberdiskurssissa nousee usein sodan määritelmä. Mikä erottaa kyberterrorismin ja sabotaasin, ja mikä sabotaasin ja tietoverkkosodankäynnin? Ensimmäistä kahta ei välttämättä erota mikään, vaan kyse on lähinnä sanavalinnasta (Kuparinen, 2009). Terrorismi määritellään Websterin sanakirjassa seuraavasti: ”terrorism: the systematic use of terror especially as a means of coercion”. Sanalle terrori taas annetaan ensisijaiseksi merkitykseksi seuraavaa: ”terror: a state of intense fear.”

Käsitteitä nettisabotaasi ja nettiterrorismi voi tällä hetkellä pitkälti käyttää ristikkäin (Kuparinen, 2009), ja kun ajatellaan esimerkiksi tyypillistä kuvausta kyberterroristien iskusta, eli esimerkiksi Viron patsaskiistan aikaisia palvelunestohyökkäyksiä mm. pankkien verkkosivuille, voidaan kysyä, oliko kyse ”äärimmäisen pelon lietsonnasta”? Tätä pohtii myös James Lewis (CSIS):

> *“Terrorism requires violence and horror. On September 11th, for example, after a day of shocking images, riders of Washington’s subway system could still smell smoke in the tunnels from the burning Pentagon. In Estonia’s recent cyber incident, people were unable to access their bank accounts online.”*

Lewis jatkaa toteamalla, että on olemassa tahoja, joiden mielestä liioittelu ”eeppisistä tuhoista” on ainoa tapa saattaa kyberuhat ihmisten tietouteen. Bendrathin (2004) ajatukset terrorismista kyberdiskurssin villinä korttina eivät siis ole kaukaa haettuja. Sanaa *terrorismi* käytetään kyberdiskurssissa löyhin perustein kertomaan toiminnasta, joka on lähempänä sabotaasia ja rikollisuutta, kuten Viron tapauksessa. Mikäli ”terrorismin” tuloksena esimerkiksi Viron lennonohjausjärjestelmät olisivat häiriintyneet ja

aiheuttaneet ihmisille hengenvaaran, sanan käytön voisi ymmärtää. Silti *The Telegraph* uutisoi 30.3.2007 seuraavalla otsikolla: ”Cyber-terrorism is real - ask Estonia.”

Oleellista ei niinkään ole se, millä nimellä media tätä toimintaa kutsuu, vaan se, mitä kyberterrorismi tarkoittaa viranomaiskielessä ja lakiteksteissä, ja kuinka suuri vaikutus medialla niihin on:

> *“Though nobody really knew how sophisticated Al Qaeda’s computer literacy was, more and more people were afraid of them. This created a kind of vicious circle, with the media dramatizing the intelligence estimates, and politicians in turn picking up media quotes.”* (Bendrath, 2005:63)

On tietenkin olemassa myös toimintaa, joka toteutuessaan voi muodostaa todellisen uhan. Kuitenkin tietoverkkosodankäynnin määritelmä on häilyvä. Milloin voimme sanoa kyberhyökkäyksen olevan sodankäyntiä, ja millä tavoin sitä vastaan on oikeutettua puolustautua?

Epäsymmetrinen sodankäynti on muodikas käsite (Yould, 2003). Kiinalle, tai mille tahansa maalle, se kuitenkin on poliittisesti ja sodankäynnillisesti tärkeä toimintatapa. Halpuuden ja etäisyyden tuoman turvallisuuden lisäksi tietoverkkosodankäynnin etuna on sen epäselvä status sodankäynnin muotona.

Tietoverkkosodankäynnin määritteleminen on oma lukunsa, mutta oleellista tämän tutkimuksen kannalta on se uhka, joka siihen eri diskursseissa liitetään. Uhka on tunne (Huhtinen, 2005, Huhtinen & Rantapelkonen, 2007), ja, toisin kuin viimeaikaisissa sodissa, kybersodan kerrotaan muodostavan lähes fyysisen uhan ulottuessaan ihmisten arkipäivään ja koteihin. Meitä jaksetaan muistuttaa sitä, ettet koskaan voi olla varma käyttääkö nettirikollinen tietokonettasi roskapostin lähettämiseen, ja että nettipankissa on riskinsä. Osaamme myös pelätä sitä, että terroristit tunkeutuvat ydinvoimalan tai sähkölaitoksen verkkoon, ja hankaloittavat kymmenien ja satojen tuhansien ihmisten arkipäivää. *The Wall Street Journal* julkaisi artikkelin nimeltä *Hiroshima 2,0*, jossa U.S. Cyber Consequences Unitin edustaja Scott Borg konkretisoi sen uhan, josta viranomaisraporteissa varoitetaan:

> *“If you shut down power for about three days, it causes very little damage. We can handle a long weekend. But if you shut down power for longer, all kinds of other things begin to happen. After about 10 days the curve levels off with about 72% of all economic activity shut down. You*

> *don't have air conditioning in the summer; you don't have heating in the winter. Thousands of people die.”*

Kiina ei vielä voi haastaa USA:ta perinteisessä sodankäynnissä, mutta tietoverkkosodankäynnin kanssa asia on toisin: hyökkääminen on helppoa ja halpaa, ja puolustautuminen sitäkin vaikeampaa ja kalliimpaa (Yould, 2003). Epäsymmetrinen sodankäynti ja sitä kautta verkkosota on terrorismin tavoin noussut omaksi kategoriakseen perinteisen sodankäynnin rinnalle (Paldanius, 2005). Kyse on siis väkivallasta ja voimankäytöstä. Traagisuudella ei enää ole sijaa länsimaisessa perinteisessä sodankäynnissä (Huhtinen, 2005: 44), mutta kyberretoriikka tuntuu tekevän poikkeuksen, sillä sen uhreja ovat amerikkalaiset itse. Siinä missä amerikkalaiset neutralisoivat sotaraportointiaan Irakin sodan aikana ja kertoivat kohteista ”systeemeinä”, kyberhyökkäys rinnastetaan hirmumyrsky Katrinaan ja terrori-iskuihin (Cybersecurity Act 2009), joiden uhreina kuoli tavallisia amerikkalaissiviilejä. Ironista on, että Irakissa USA:n iskut sähkövoimaloihin olivat siviilejä säästäviä ”täsmäiskuja”, mutta epäily hakkereiden murtautumisesta USA:n sähkölaitoksen järjestelmään aiheuttaa spekulaation tuhansista mahdollisista kuolonuhreista.

Mitä meidän sitten halutaan pelkäävän? Median esittämiä uhkia (kriittisen infrastruktuurin sabotoiminen, vakoilu, jne.) ei välttämättä miellä väkivallaksi, mutta silti ne uutisoidaan sellaisena: ”China’s cyber army is preparing to march on America, says Pentagon” (*Times Online*, 8.9.2008), tai: ”Spy chiefs fear Chinese cyber attack” (*Times Online*, 29.3.2009), sekä: ”Beware: enemy attacks in cyberspace” (*Financial Times*, 3.9.2007).

On selvää, että kyberdiskurssi elää omaa erillistä elämäänsä, jolla on omat motiivinsa. Todellisia uhkia ja riskejä ei popularisoida medioille, vaan *cyber* merkitsee diskurssissa ennemminkin salattua agendaa, mm. turvallistamista, kuin terrorismia tai vihollisia. Seuraava luku tarkastelee kyberdiskurssia informaatio-operaationa sekä sen yhteiskunnallista merkitystä.

3. POLITIIKKAA, TURVALLISUUTTA, VALLANKÄYTTÖÄ?

Kyberdiskurssin rooli informaatiosodankäynnin osana on samanlainen kuin muunkin turvallisuusdiskurssin: valtion hegemonian vahvistaminen ja perusteleminen. Kybersodan status sodankäynnin muotona on kuitenkin ollut hyvin häilyvä. Mitä kyberdiskurssilla halutaan saavuttaa?

Tietoverkko-operaatioissa kyse on vallan hankkimisesta ja käyttämisestä. Nopea vilkaisu mediaan ja viranomaisraportteihin kertoo kyberdiskurssin sisältävän käsitteitä kuten *turvallisuus, tieto, kilpajuoksu, asevarustelu, uhka* ja *pelote*. Tiedon noustua aseeksi se on myös uusi uhka, jolloin taito hankkia tietoa on valtaa. Tällä on perusteltu Kiinan muodostamaa uhkaa: vaikka se ei pystyisi haastamaan esimerkiksi USA:ta perinteisessä sodankäynnissä, se on USA:lle valtava kyberuhka. Autoritäärinen sotilasvalta voi värvätä haluamansa kansalaiset töihin vaikkapa ilmaiseksi samaan aikaan kun USA:ssa taistellaan laman, matemaattisten aineiden kurjistuvien arvosanojen ja pienenevien opiskelijamäärien kanssa. Pentagon nimeää tiede- ja teknologia-alan koulutuksen taantumisen suurimmaksi pidemmän aikavälin uhaksi, sillä 1,3 miljardilla asukkaallaan Kiinalla on myös tilastollisesti enemmän huippulahjakkuuksia käytössään (Yhdysvallat, 5.10.2007). Kiinan ja USA:n resurssit ovat hyvin erilaiset. USA on haastettu kalliiseen suojautumissotaan, minkä takia USA on aloittanut tehokkaan turvallistamiskampanjan. Toisin sanoen, ei riitä että vastatoimet kohdistuvat vastustajaan, vaan sen lisäksi kotimaan yhteiskunta joutuu informaatio-operaation kohteeksi. Tilannetta ei helpota maailmantalous, eikä Kiinan niskalenkki Yhdysvaltojen suurimpana velkojana (Tuohinen, 2009).

3.1. Ennaltaehkäisevät verkkoiskut – voidaanko tietoverkkosotaan lähteä kuin Irakiin?

Tietoverkkosodankäyntiin liittyvä diskurssi on perinteisesti noudattanut roolijakoa, jossa hyökkäävää osapuolta on kuvailtu rikollisena, terroristina, tai salassa pysyttelevänä mutta kyseenalaisesti toimivana valtiona. Vaikka kaikki tietävät ja toteavat tietoverkkosodankäynnin olevan arkipäivää, olisi hyvin epätavallista käydä avointa keskustelua siitä vaihtoehdosta, että hyökkäys olisi hyväksyttävä keino puolustautua tai ajaa valtion intressejä. Lokakuussa 2008 Yhdysvaltain puolustusministeri Robert M. Gates totesi, että tulevaisuuden hallintojen täytyy pohtia sitä, minkä tasoista hyökkäystä voidaan pitää sodankäyntinä, ja millä tavalla siihen on sopivaa vastata (Yhdysvallat, 28.10.2008).

Hyökkäyksen sisällyttämistä tietoverkkosodankäynnin doktriiniin pohdittiin syksyllä 2009 julkaistussa raportissa (Owen, Dam & Lin, 2009). Sen mukaan olisi luontevaa, että tietoverkkohyökkäykset olisivat osa USA:n asevoimien doktriinia. Tämänhetkinen USA:n sotilasdoktriini tunnistaa tietoverkkohyökkäykset ja -operaatiot, joiden kautta joko häiritään, estetään ja tuhotaan tietoa, tietoverkkoja ja tietokoneita, puolustetaan ja suojataan niitä, tai kerätään niistä tietoa. Sama doktriini toteaa, että kaikkia näitä keinoja voidaan käyttää sekä hyökkäyksellisesti että puolustuksellisesti, vaikka virallinen kanta tietoverkkohyökkäyksen suorittamiseen on epäselvä.

Eri puheissa esiintyneet ilmaisut *pelote* ja *varustelukilpa* viittaavat siihen, että ennaltaehkäisevä hyökkäys olisi doktriinin mukainen paitsi perinteisessä sodankäynnissä, myös tietoverkoissa. James E. Cartwright, Commander of U.S. Strategic Command, toteaa raportissa seuraavaa:

> *"If we apply the principles of warfare to the cyber domain, as we do to sea, air and land, we realize the defence of the nation is better served by capabilities enabling us to take the fight to our adversaries, when necessary to deter actions detrimental to our interests."*

Toisin sanoen, sen sijaan että miettisimme yksin tietoverkkohyökkäykseltä puolustautumista, tai tapaa jolla siihen olisi sopivaa vastata, meidän tulisi pohtia doktriinia ja käydä keskustelua siitä, salliiko doktriinimme tai maan lainsäädäntö hyökkäyksen tekemisen, ja millä ehdoilla. USA:ssa on herätty siihen, että amerikkalaiset eivät voi sanella sodankäynnin kulkua kuten ennen. Informaatioylivallan menetys tarkoittaa aloittellisuuden muttumista reaktiivisuudeksi (Daniel Ventre, 2009). Juuri tätä on käytetty argumenttina, kun kiinalaista kyberdoktriinia on kuvattu aloitteellisuuteen perustuvana.

Tähänastiset kyberhyökkäykset on tähän asti julkisesti tuomittu, ja suuria kyber-resursseja hallussaan pitäviin maihin, kuten Kiinaan ja Venäjään, on perinteisesti suhtauduttu varauksella. Owen, Dam & Lin (2009) luettelevat raportissaan kuitenkin mahdollisuuksia, joissa tietoverkkohyökkäystä voisi hyödyntää informaatio-operaationa. Väärän tiedon levittämisen, psykologisten operaatioiden ja elektronisen sodankäynnin lisäksi mainitaan harhauttaminen, joka voitaisiin toteuttaa esimerkiksi valheellisilla sähköposteilla. Lisäksi hyökkäyksiä voisi tehdä perinteisen sodankäynnin tukena DOS-hyökkäyksinä sekä vastapuolen komento- ja hallintajärjestelmiin tunkeutumalla. Kaikki edellä mainitut keinot ovat niitä samoja, jotka esiintyvät amerikkalaisessa kyberdiskurssissa amerikkalaisiin kohdistuvina uhkakuvina. Julkisissa viranomaisraporteissa keskustelua on käyty lähestulkoon ainoastaan puolustuksellisesta sodankäynnistä, siihen

liittyvästä lainsäädännöstä ja taloudellisista resursseista. Millään suurvallalla tuskin on kuitenkaan varaa jättää muitakin tietoverkkosodankäynnin mahdollisuuksia hyödyntämättä.

3.2. Yhteiskunta ristitulessa

Sodat ja kriisit ovat tuoneet tullessaan uusia lakeja ja rajoituksia. Syyskuun terrori-iskujen jälkeen säädettiin USA Patriot Act, jota seurasi Department of Homeland Securityn perustaminen. Kumpaakin uudistusta on arvosteltu tehottomuudesta. Kritiikkiä saa myös Cybersecurity Act of 2009. Lakialoitetta kritisoidaan turvallisuuden ja yksityisyyden rappeuttamisesta:

> *"One proposed provision gives the President unfettered authority to shut down Internet traffic in an emergency and disconnect critical infrastructure systems on national security grounds goes too far. Certainly there are times when a network owner must block harmful traffic, but the bill gives no guidance on when or how the President could responsibly pull the kill switch on privately-owned and operated networks." (Granick, 10.4.200)*

Turvallisuusteknologian asiantuntija Bruce Schneier toteaa *Wall Street Journalissa*, ettei kyberturvallisuus ole asevoimien tai edes hallituksen ongelma, vaan globaali haaste. Hallituksen ongelmiksi nimetään kuitenkin hyvin arkipäiväisiä asioita:

> *"GAO reports indicate that government problems include insufficient access controls, a lack of encryption where necessary, poor network management, failure to install patches, inadequate audit procedures, and incomplete or ineffective information security programs. These aren't super-secret NSA-level security issues; these are the same managerial problems that every corporate CIO wrestles with." (Wall Street Journal,* 31.3.2009)

Herää kysymys, että mikäli tietoturvallisuusongelmat kiteytyvät muun muassa virkamiesten hankaluuksiin ohjelmistojen käytön kanssa, onko kansalaisten yksityisyyden tai vapauden rajoittaminen tehokas ase tietoturvallisuuden parantamisessa? Lakiuudistukset ja byrokraattiset uudelleenorganisoinnit ovat esimerkki ajattelutavasta, että *jotakin on tehtävä*. Toiminnan korostamiseen palataan luvuissa 4 ja 5, sillä ne näyttelevät poliittisessa diskurssissa tärkeää osaa.

Turvallistamispolitiikan kriitikot ovat huolissaan siitä, että samalla kun hallitukset ja poliittiset elimet haluavat todistaa toimintakykynsä ja aloitteellisuutensa uudistamalla lainsäädäntöä, rajoitusten vaikutuspiiriin jää vain tavallisia kansalaisia, jotka joutuvat tinkimään vapaudestaan. Tietoverkkosodankäynnin diskurssissa liikutaan hyvin lähellä länsimaisia perusarvoja, kuten sananvapautta, tiedonvälitystä ja viestintäsalaisuutta, eikä huoli niiden vaarantumisesta ole aiheeton.

Huoli kansalaisten vapaudesta ei rajoitu ainoastaan Yhdysvaltoihin. Turvallisuutta koskeva eurooppalainen tutkimusohjelma (European Security Research Programme, ESRP) saa kritiikkiä Ben Hayesin *Neoconopticon*-raportissa. Hayesin mukaan pieni aseteollisuuden edustajien ryhmä on kaapannut EU:n turvallisuuspolitiikan teon yksityiselle sektorille vain näennäisen demokraattisin keinoin. Yhteiskunnan muuttuminen valvontayhteiskunnaksi vauhdittuu yksityisen sektorin hyötyessä siitä taloudellisesti, ja Hayes peräänkuuluttaakin valvonnan rajoittamista.

> *"It is not just a case of "sleepwalking into" or "waking up to" a "surveillance society", as the UK's Information Commissioner famously warned, it feels more like turning a blind eye to the start of a new kind of arms race, one in which all the weapons are pointing inwards."*
> (Hayes, 2009)

Hayes sivuaa raportissaan myös uhkakuvia. EU:ssa on Yhdysvaltojen tapaan vallalla uhkadiskurssi, jossa perustellaan Homeland Security -politiikkaa ulkoista uhkaa vastaan.

> *"The entire homeland security paradigm is predicated on the idea that western nations face an unprecedented threat to their 'way of life'. Be it pandemics, political violence or protest, the 'problem' is seen as a grave danger and the 'solution' couched in terms that favour the transfer of social policy responses from civilian agencies to law enforcement and militarist proscriptions developed by securocrats and technocrats. This process feeds on much of the recent discourse on globalisation, which asserts that western states, far from becoming more authoritarian and militarised as they plainly are, must defend their 'way of life'. This rhetoric must be challenged head on. There are, of course, genuine threats to security, but all sense of proportion appears to have been lost. In a troubled and desperately unequal world, Europe is already relatively secure."* (2009: 80).

Hayesin mukaan keksityt ja todelliset uhkakuvat ylläpitävät tarvetta uudelle turvallisuuspolitiikalle (2009:79). Kysymys on siis maailmanlaajuisesta ilmiöstä, jonka ensimmäisiä uhreja ovat kansalaiset ja yhteiskunnat. Kompromissit yksityisyyden ja vapauden rintamalla ovat turvallisuus- ja turvallistamisdiskurssin väistämätön lopputulos. Uhkakuvien varjolla saadaan läpi ikäviäkin muutoksia.

3.3. Valta ja väkivalta kyberdiskurssissa

Kyberdiskurssi on ristiriitaista. Yhtäällä kerrotaan meitä uhkaavasta vaarasta, kuten ”elektronisesta Pearl Harborista”, ”Cyber Katrinasta” ja ”Hiroshima 2,0:sta”. Toisaalla pohditaan oman toiminnan laajentamista offensiiviseen suuntaan. On vaikeaa käsitystä siitä mitä on normaalitila, ja milloin olemme vallan tai väkivallan kohteena. Kuten aikaisemmin todettiin, on vaikeaa tietää milloin olemme todellisen kyberhyökkäyksen kohteena, ja milloin kertomukset hyökkäyksestä ovat osa yhteiskuntaan kohdistuvaa informaatio-operaatiota, tai mahdollisesti median tulkintaa aiheesta. Viranomaiset kiirehtivät julkaisemaan raportteja, jotka päättyvät aina suosituksiin siitä, mitä *pitäisi tehdä.*

Pahin syytös kriisin sattuessa on se, että siihen ei reagoitu, tai asian hyväksi ei tehty tarpeeksi. Poliitikoilta ja viranomaisilta odotetaan ehdotuksia ja näkemyksiä, ja todellinen ongelma uhkaa jäädä sivuseikaksi. Slavoj Zizek (2009) toteaakin, että tällä hetkellä uhkana ei ole ihmisten passiivisuus, vaan pseudo-aktiivisuus - vaatimus ”aktiivisuudesta” ja ”osallistumisesta”:

> *”People intervene all the time, ‘do something’; academics participate in meaningless debates and so on. The truly difficult thing is to step back, to withdraw. Those in power often prefer even a ‘critical’ participation, a dialogue, to silence – just to engage us in ‘dialogue’, to make sure our ominous passivity is broken.”*

Toimintakeskeisyys on osa länsimaista “just do it” -ideologiaa, jossa ihminen voi säädellä elinympäristöään ja muokata siitä aktiivisella toiminnalla haluamansa kaltaisen. Mikäli johtajalla ei ole kertoa toimintasuunnitelmaa kriisin hetkellä, hän on arvoton. On parempi toimia ja epäonnistua, kuin jättää toimimatta. Koska toimintaa odotetaan, myös turvallistaminen on helppoa. Voi olla etteivät turvallisuustoimet tee elämästämme yhtään turvallisempaa, mutta voidaanko ne jättää tekemättä, mikäli ne ovat ainoa ehdotus tilanteen korjaamiseksi? Kukapa haluaisi olla se, joka kannattaa riskinottoa, jota odottaminen ja toimimattomuus yhteiskunnassamme edustavat. Korvikeratkaisut hyväksytään, koska silloin yhteiskunnalla on tunne siitä, että jotain on edes yritetty tehdä. James

Fallowsin kritiikki kuvaa hyvin turvallistamistarpeen seurauksena nopeasti läpiajettua Homeland Security-uudistusta:

> *"The Department of Homeland Security should not exist. Its rushed, bipartisan creation in 2002 reflected the political imperative to do something in response to disaster, whether or not that something made sense." (See also: case for the Iraq War.)* (Fallows, 2009)

Tämä kritiikki sopii hyvin myös kyberdiskurssiin. Zizek (2009:34) toteaakin, että ainoa tapa saada ihmiset toimimaan on pelko. Pelosta ja pelottelusta on tullut osa politiikkaa. Tämä yhdistettynä diskurssiin muodostaa tehokkaan retoriikan ja vallankäytön muodon – uhkakuvat. Uhkakuvat sisältävät paitsi ajatuksen siitä mikä (toiminta) meitä uhkaa, myös vaatimuksen siitä mitä meidän tulisi tehdä.

Zizek (2009) lähestyy väkivallan käsitettä kielen kautta ja argumentoi sen olevan ehdottoman vallankäytön ja väkivallan väline. Kommunikaation tärkeyttä korostavassa länsimaisessa kulttuurissa kieli myös jakaa ihmiset eri maailmoihin ja todellisuuksiin. ”Verbaalinen väkivalta ei ole toissijaista vääristymää, vaan keino johon kaikki inhimillisen väkivallan muodot turvautuvat. (2009:57)” Kielen väkivalta on vallankäyttöä. Zizek tunnistaa ei-fyysisen väkivallan synnynnäisenä osana ”systeemiä”, joka ylläpitää valtasuhteita ja väkivallan uhkaa. Näin ollen vallankäyttöön pyrkivää, ”omille” suunnattua diskurssia voidaan pitää väkivaltana. Kyberdiskurssi ylläpitää väkivallan uhkaa, ja informaatio-operaationa sen vaikutuskentässä ei ole ainoastaan vastapuoli, vaan myös ”me”.

Seuraavassa luvussa rakennetaan metodi, jonka avulla puretaan kielen sisältämiä uhkakuvia. Huomio kiinnittyy erityisesti tässä kappaleessa esiin nousseisiin tekemisen kuvauksiin. Koska omaa identiteettiä, arvoa ja asemaa määritellään tekemisen kautta, tulee huomiota kiinnittää myös siihen, millä tavalla vastapuolta kuvataan.

4. LINGVISTINEN VIITEKEHYS JA METODOLOGIA

Mikäli halutaan tutkia turvallisuuskäsitystä, täytyy ensin selvittää millaisista uhkatekijöistä diskurssi koostuu. Käsitteellä ”uhka” viitataan tässä tutkimuksessa ns. eksistentiaaliseen uhkaan. Diskurssin analysoija ei kuitenkaan tee päätöstä siitä, kuvataanko jokin uhka eksistentiaalisena vai ei. Tästä määritelmästä vastaa turvallistaja (Buzan, Waever & de Wilde, 1998).

Turvallistaminen on usein lähes puhtaan lingvistinen prosessi. Siinä on kyse informaatio-operaatiosta, jossa yleisölle pyritään antamaan vaikutelma turvallistajan määrittelemästä uhasta. Turvallistaja on siis tässä diskurssissa vallankäyttäjä, jonka tehtävänä on voittaa puolelleen kuulijoidensa ”sydämet ja mielet” (Butt, Lukin & Matthiessen, 2004).

Tässä luvussa esitellään joukko lingvistisiä teorioita ja viitekehyksiä, joiden pohjalta lopullinen tutkimusviitekehys muodostuu. Pääpaino on systeemis-funktionaalisella kieliteorialla sekä siihen tukeutuvalla Appraisal-teorialla, joilla avataan kielen rakenteita ja merkityssuhteita. Rinnalla sivutaan suppeampia diskurssianalyysimetodeja, sekä turvallistamisprosessin tutkimusta varten kehitettyä konstruktivistis-operationaalista metodia, jonka pyrkimyksenä on määrittää turvallistamisen diskurssi politisoinnista erillisenä diskurssina.

Ihmisen kokema uhka liittyy ensisijaisesti siihen, kuinka häntä kohtaan toimitaan ja mitä hänelle tuon toiminnan seurauksena tapahtuu. Tämä tarkentaa tutkimuskysymyksiä:

- Miten ’meitä’ uhataan?
- Miten ’he’ toimivat: mitä ’he’ tekevät ja millaisia ’he’ ovat?

Nämä kysymykset kiinnittävät päähuomion tekemisen kuvauksiin, eli verbeihin. Niinpä tutkimusmetodit rakentuvat juuri näiden prosessikuvausten ympärille.

4.1. Systeemis-funktionaalinen kieliteoria

Kysymyksiä kielen rakenteen ja tulkinnan suhteesta voidaan lähestyä systeemis-funktionaalisen kieliteorian (Systemic-Funtional Linguistics, SFL) kautta. Se nimeää kielelle kolme merkitystasoa (metafunktiota):

1. Eksperientiaalinen merkitys eli maailmankuvan selittäminen. Tämä merkitystaso käsittää mm. asioiden nimeämisen sekä prosessien (eli

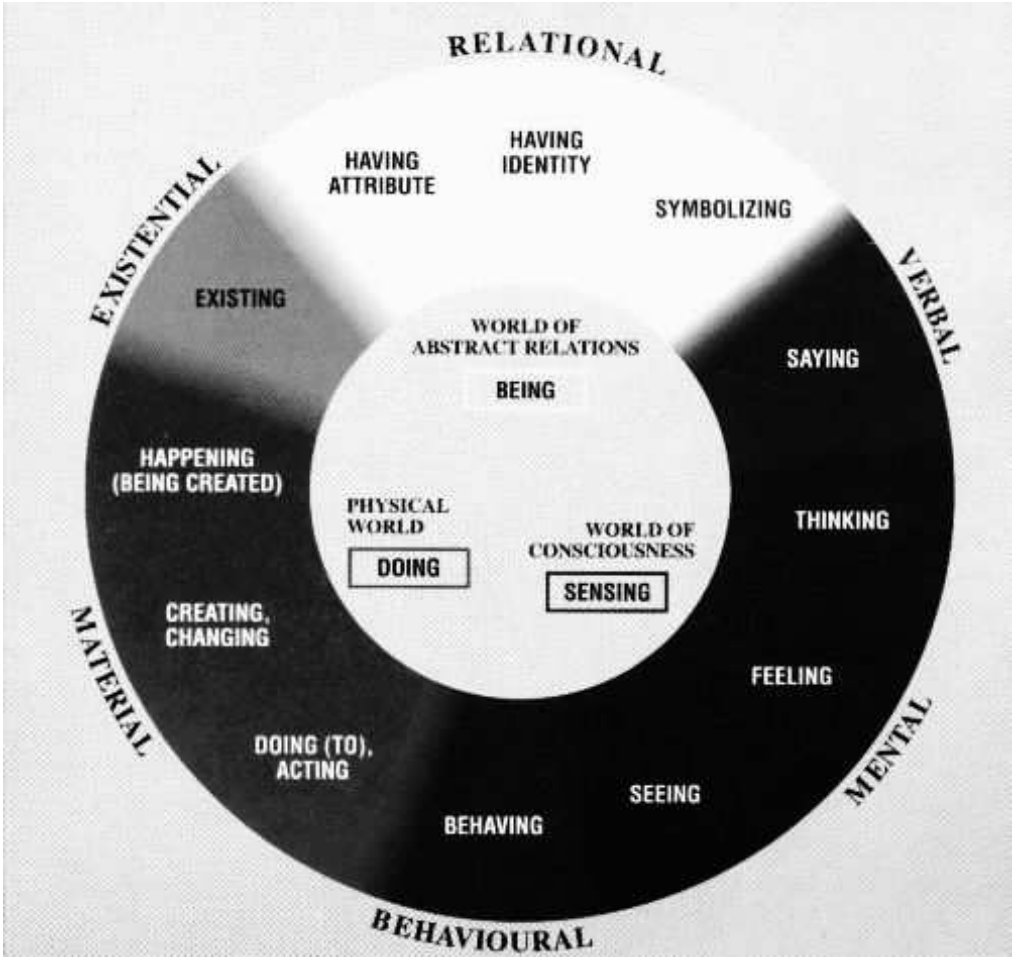
tekemisen) nimeämisen.
2. Interpersoonainen merkitys, eli kielen tunnistaminen vuorovaikutukseksi. Tällä merkitystasolla analysoidaan kielen modaalisuutta, eli puhuja-asenteisuutta, ja se sisältää kuvaukset viestijästä ja viestin vastaanottajasta.
3. Tekstuaalinen merkitys, eli kielen informaatiorakenne. Tekstuaalisuus tekee kielestä koherenttia ja ymmärrettävää.

Tässä tutkimuksessa oleellisiksi merkitystasoiksi nousevat eksperientiaalinen ja interpersoonainen taso, sillä tarkoituksena on selvittää miten eri tahojen toimintaa kuvataan, ja millaisia osapuolia toimintaan ja diskurssiin sisältyy.

Systeemis-funktionaaliseen kieliteoriaan sisältyy ajatus siitä, että kielellisillä valinnoilla toteutamme verbaalisesti omaa ideologiaamme. Esimerkiksi sana- ja rakennevalinnoilla voidaan vaikuttaa viestin ymmärtämiseen. Jos toistamme tutkimuskysymyksen ”Millaisen toiminnan tekijä osapuoli on?” ja tutkimme seuraavia esimerkkejä, on helppo huomata miten eri prosessityypeillä voidaan viestiä merkityseroja:

A: Verbaalinen	*He kertovat olevansa syyttömiä.* *He väittävät olevansa syyttömiä.*
B: Mentaalinen	*He uskovat olevansa syyttömiä.* *He kuvittelevat olevansa syyttömiä*
C: Relationaalinen	*He ovat syyttömiä.* *He eivät ole syyttömiä.*

Kuten esimerkeistä voi huomata, ei ole yhdentekevää millä sanoin tekemistä kuvataan. Esimerkkilauseiden tulkittavuus riippuu pitkälti siitä, mitä prosessityyppiä siinä käytetään, eikä ole liioiteltua sanoa lauseen merkityksen rakentuvan juuri prosessin ympärille. Voidaan esimerkiksi sanoa, että kun kuvataan jotakin muuta kuin omaa toimintaa mentaalisella prosessilla, lause muuttuu väitteeksi ja kannanotoksi. Relationaalisella prosessilla taas ”kerrotaan tosiasioita”, joko jonkin asian olemassaolosta, tai siitä, ettei jotakin asiaa ole suhteessa toiseen.



Kuva: Prosessityypit Hallidayn (2004) mukaan.

Prosessityypeillä on seuraavia merkityksiä:

1. Materiaaliset prosessit: Usein ns. tekemisen ja tapahtumisen kuvauksia, kuten *lyödä, osua, kiivetä, räjäyttää, muuttaa, kasvaa.*
2. Mentaaliset prosessit: Kognition, havainnoinnin ja esimerkiksi arvostamisen kuvauksia, kuten *pitää, tietää*, *tuntea*, *ajatella.*
3. Relationaaliset prosessit: Kertovat asioiden suhteista, esim. X = Z, tai omistamista. Relationaaliset prosessit voivat myös luokitella intensiivisiksi (*vihollinen on paha*) tai possessiivisiksi (*vihollisella on pahoja aikomuksia*). Relationaaliset prosessikuvaukset identifioivat, luonnehtivat ja kuvaavat.
4. Eksistentiaaliset prosessit: Kertovat asioiden olemassaolosta. Englannin kielessä ilmaistaan usein *there is* -rakenteella eli ns. muodollisella subjektilla.
5. Behavioraaliset prosessit: Kuvaavat käyttäytymistä. Tätä prosessiluokkaa on joskus vaikea erottaa materiaalisesta tai mentaalisesta. Behavioraaliset prosessit voivat olla sanoja kuten *itkeä, pyörtyä, iloita.*
6. Verbaaliset prosessit: Kertovat verbaalisista teoista, kuten *sanoa,*

kertoa, puhua, ilmoittaa.

Sotaretoriikassa ja informaatio-operaatioissa eri prosessityypeillä on omat tehtävänsä. Yleisesti voidaan sanoa, että materiaaliset, verbaaliset, relationaaliset ja eksistentiaaliset prosessit ’kertovat tosiasioista’, sillä ne ovat mahdollisesti todistettavissa olevia eivätkä yleensä sisällä analyysia toisesta osapuolesta. Sen sijaan mentaaliset prosessit ovat aina tietynlaisen analyysin tulosta ja väitteitä toisen osapuolen yksityisten, pään sisäisten tapahtumien tulkinnasta. Hallidayn (2004) mukaan mentaaliset prosessit kuvaavat ”tiedostamisen maailmaa” (*world of consciousness*), jonka sisällöstä ulkopuolisella ei voi olla varmaa tietoa. Niinpä esimerkiksi sotaretoriikassa vihollisen ajatuksista kertominen on aina ideologisesti värittynyttä ja vahva kannanotto – sillä eihän ulkopuolinen voi kuin spekuloida toisen osapuolen tunnetiloja tai haluja:

> *“We love the idea of people being able to freely debate issues. We love freedom, and these cold-blooded killers hate freedom. And that's why they want to come and hurt America. And we are not going to let them.”* (President G. W. Bush, 19.6.2002)

SFL tarjoaa siis tähän tutkimukseen eksperientaalisen ja interpersoonaisen metafunktioiden käsitteet, sekä viitekehyksen prosessittyyppien analyysille. Tätä metodistoa täydentää seuraavan kappaleen Appraisal-teoria.

4.2. Evaluaatio diskurssissa: Asenteen sanallistaminen

Evaluaatiota voi lähestyä tutkimalla identiteetin, toiminnan, normien, aseman ja voimavarojen kuvaustapoja.

> *[…]when we examine discourses that generally function as modes of self-defence, legitimation, or explanation, or that have other self-serving functions, we would typically expect a prominent presence of meanings that can be interpreted as expressions of such categories.* (van Dijk, 1995: 147)

Nämä eri kategoriat on tiivistetty seuraavaan taulukkoon, joka on muotoiltu van Dijkin (1995:147-149) mukaan:

Oman identiteetin kuvaukset:	Yleensä positiivisia kuvauksia, jotka vastaavat kysymyksiin kuten *ketä me olemme* ja *millaisia olemme*. Nämä identiteettikuvaukset ovat tyypillisiä vähemmistöjen keskuudessa, sekä dominanssinsa uhatuksi tuntevien ryhmien diskurssissa.
Tekemisen kuvaukset:	Tekemisen kuvaukset vastaavat kysymyksiin *miten me toimimme* ja *mikä on tehtävämme*. Nämä kuvaukset ovat tyypillisiä niiden ryhmien keskuudessa, joiden toimintatavat ovat niiden olemassaolon kannalta tärkeitä (asiantuntijat, ammattilaiset, aktivistit).
Normi- ja arvokuvaukset	Normi- ja arvokuvaukset määrittelevät sen, mitä “me” pidämme oikeana tai vääränä, hyvänä tai huonona, tai kunnioitettavana tai häpeänä. Näitä määritelmiä vastaan toimivat kuvataan ulkopuolisiksi tai viholisiksi.
Aseman ja suhteiden kuvaukset:	Joskus ryhmät ja yksilöt määrittelevät itsensä suhteessa muihin osapuoliin. Identiteetti määritellään vertailun avulla.
Resurssien kuvaukset:	Ihmiset joko puolustavat resursseja tai toimivat saadakseen niitä haltuunsa. Resurssit voivat olla esimerkiksi tietoa, statusta, arvovaltaa, omaisuutta, tai mitä tahansa millä on välineellistä hyötyä. Resurssikuvauksiksi kutsutaan niitä semanttisia strategioita joilla puolustetaan resursseja tai hyökätään niiden toivossa. Joskus resurssit kuvataan osaksi identiteettiä.

Tarvitsemme siis tiedon siitä, *kuka* tekee ja *kuinka*, sekä *millainen* tekijä on (ominaisuudet, arvot, suhteet, resurssit ja potentiaali). Näihin kysymyksiin voidaan vastata systeemis-funktionaalisen kieliteorian sekä siihen tukeutuvan Appraisal-viitekehyksen avulla.

Appraisal-teoria keskittyy diskurssin semanttiseen analyysiin, eli niin sanottuun evaluaatioon. Evaluaatiolla tarkoitetaan havaintojen ja aistimusten kielellistä ilmaisua ja kuvailua. Hunston (Hunston & Thompson, 2000: 14) määrittelee ”hyvän” ja ”pahan” tavoitteiden ja päämäärien kautta. Ne asiat, jotka edistävät tavoitteiden toteutumista ovat hyviä, kun puolestaan tavoitteiden esteisiin liittyvät asiat ovat pahoja. Myös Fairclough (2003: 177) määrittelee evaluaation attribuutit niiden suotavuuden ja miellyttävyyden mukaan. Kuitenkin nämä näkemykset ovat hyvin subjektiivisia, eivätkä ne jäsenny selkeäksi viitekehykseksi. Hunston & Thompson (2003: 13) toteavatkin, että evaluaatiossa kyse on vertailun, subjektiivisuuden ja sosiaalisen arvonannon signaalien tunnistamisesta.

Martin & White (2005: 7) ovat jäsentäneet pitkälle viedyn Appraisal-teorian evaluaation analysoimiseksi. Se toimii osana SF-kieliteoriaa, sillä se toimii diskurssin interpersoonaisen merkityksen piirissä, eli tutkii ”sosiaalisten suhteiden rakentamista” (Martin & White, 2005: 7).

Evaluaation kautta tapahtuva arvottaminen (*value assignment*) on yksi tapa viestiä identiteettiä diskurssissa.

Evaluaatiolla on kolme tehtävää (Hunston & Thompson, 2000: 6). Ensimmäinen niistä on puhujan mielipiteiden ja arvomaailman viestiminen. Toiseksi, se jäsentää diskurssia luomalla selkeyttä viestityn asian sisältöön. Kolmanneksi, se muokkaa puhujan ja kuulijan välistä suhdetta. Koska kaikki viestintä on kohdennettu jollekin toiselle osapuolelle, sisältää diskurssi vihjeitä puhujan ja kuulijan välisestä suhteesta. Tämä toimii kontekstina viestin semanttiselle tulkinnalle. Näin ollen puhujan ja yleisön välinen suhde on retoriikantutkimuksen kannalta mielenkiintoinen. Jotta yleisön vakuuttaminen onnistuisi, täytyy viestijän esiintyä tarpeen tullen asiantuntijana, auktoriteettina, tai esimerkiksi tahona, johon kuulija voi samaistua:

> *"[W]hen speakers/writers announce their own attitudinal positions they not only self-expressively 'speak their mind', but simultaneously invite others to endorse and to share with them the feelings, tastes, or normative assessments they are announcing. Thus declarations of attitude are dialogically directed towards aligning the addressee into a community of shared value and belief."* (Martin & White, 2005: 95)

Julkiset kannanotot ovat siis strategiaa sisäpiiriläisten ja ulkopuolisten määittelemiseksi.

Tämän tutkimuksen kannalta kenties hedelmällisin Appraisal-teorian osa-alue on diskurssin asennetta (*attitude*) viestivien rakenteiden tutkiminen. Diskurssissa asenne välittyy erilaisten tunteiden kuvausten kautta. Nämä kuvaukset voidaan luokitella kolmeen tyyppiin (Martin & White, 2005): tunnekuvauksiin (*affect*) sekä tuominnan (*judgment*) ja arvostuksen (*appreciation*) ilmaisuihin. Voidaan huomata, että nämä vastaavat mentaalisia ja behavioraalisia prosesseja Hallidayn (2004) SF-teoriassa. Ne siis paljastavat viestijän subjektiivisuuden, esimerkiksi ”me” vs. ”te” – vastakkainasettelun ja polarisaation, ja niiden kautta on mahdollista lähestyä diskurssin henkilökohtaisia tarkoitusperiä. Asenneanalyysin lisäksi Appraisal-teoriaan lukeutuvat vuorovaikutus- (*engagement*) ja vertailtavuusperspektiivit (*graduation*).

Appraisal-teoria mahdollistaa syvällisen evaluaatioanalyysin antamalla työkalut tutkia sanavalintaa esimerkiksi vihollista demonisoivassa tai toimintaa legitimoivassa diskurssissa. Se antaa tutkimukselle viitekehyksen, jonka avulla voidaan tutkia kuinka sanavalinta ja rakenteet vaikuttavat diskurssin informaatiosisältöön. Seuraavat kappaleet esittelevät Appraisal-teorian pääpiirteet ja tutkimuksen kannalta oleelliset teoreettiset viitekehykset.

4.2.1. Appraisal-kategoriat

Affect eli *tunnekuvaukset*

Tunnekuvaukset sisältävät sekä positiivisten että negatiivisten tunteiden ja reaktioiden kuvaukset (Haddington, 2005: 63, Martin & White, 2005: 42). Ilmaisut kuten *ilo, onni, viha* ja *sydänsuru* johtavat diskurssin emotionaaliseen ulottuvuuteen. Ne voivat esiintyä tekstissä määritteenä *(kiitollinen kansa, kansa oli kiitollinen*), prosessina (*terrorisoi kansaa*), tai ”kommenttina” (*Surullista kyllä, uhreilta ei vältytty*) (Martin & White, 2005: 45-46). Tulee huomata, että erilaisilla rakennetyypeillä on myös merkityseroja. Kun esimerkiksi verrataan ilmaisuja *kiitollinen kansa* ja *kansa oli kiitollinen*, viestii ensimmäinen pysyvää ominaisuutta, ja toinen hetkellistä mielentilaa.

Martin & White (2005: 46-49), jakavat tunnekuvaukset kolmeen kategoriaan, jotka on kuvattu seuraavaan taulukkoon:

Kategoria	Kuvaus	Sanasto
Onnellisuus/onnettomuus	”sydämen asiat”	viha, rakkaus, pitää, halveksia
Tyytyväisyys/tyytymättömyys	lopputuloksen arviointi	tylsä, kiittää, suositella
Varmuus/epävarmuus	hyvinvointi ja sosiaalinen identiteetti	luottaa, arvostaa, pelko

Judgment eli *tuominta*

Judgment eli 'tuominta' kuvaa asenteitamme ihmisiin ja heidän käytökseensä (Martin & White, 2005: 52). Martin & White erottavat ‘sosiaalisen kunnioituksen' (*social esteem*) ja 'sosiaalisen hyväksynnän '(social sanction). Sosiaalinen kunnioitus sisältää normaaliuden, kapasiteetin ja sinnikkyyden käsitteet ja se toimii sosiaalisten verkostojen kontekstissa, kun taas sosiaalinen hyväksyntä keskittyy rehellisyyden, kunniallisuuden ja eettisyyden ilmaisuun, jotka on tyypillisesti kirjattu lakeihin, sääntöihin ja normeihin (Martin & White, 2005: 52).

Kuten tunnekuvauksetkin, tuominta voi olla positiivista tai negatiivista. Kielen modaalisuus mahdollistaa lisäksi tuominnan tason vertailun. Seuraavista esimerkeistä kohta C viestii voimakkainta modaalisuuden tasoa, A:n ollessa heikoin.

A) Sinä voit käyttäytyä kunniallisesti. B) Sinun pitäisi käyttäytyä kunniallisesti. C) Sinun täytyy käyttäytyä kunniallisesti.

Esimerkin kaltainen modaalisuuden arviointi yhdistää tämän Appraisal-teorian osa-alueen kieliopilliseen, systeemis-funktionaaliseen analyysiin.

Appreciation eli *arvostus*

Martin & White (2005:56) rajaavat arvostuksen määritelmän siihen, millä tavoin ilmaisemme arvostustamme ympärillämme olevia asioita kohtaan. Kuten tunnekuvaukset ja tuomintakin, arvostuksen kuvaukset jakautuvat omiksi alatyypeikseen. Reaktiot (*Vihasin sitä, Se oli hieno*), kuvailu (*tyylikäs, vakaa*), ja arvokuvaukset (*arvokas, tärkeä*) voivat olla joko positiivisia tai negatiivisia.

4.2.2. Kiertoilmaukset, evaluaatio, sekä "epäevaluaatio"

Aina ei ole selvää lukeutuuko diskurssin sisältö tunnekuvaukseksi, tuominnaksi vai arvosteluksi, sillä ihmiset käyttävät metaforia ja esimerkiksi sarkasmia diskurssissaan. Diskurssin tulkitsija tulkitsee tekstiä heidän kognitiivisen ja emotionaalisen tietotasonsa mukaan, jolloin ns. rivien välistä lukeminen mahdollistuu ilman suoranaisia tunne-, tuominta- tai arvostuskuvauksia. Leksikaalisesti tulkittuna *hän kyynelehti,* on neutraali ilmaisu. Semanttisesti näin ei ole.

Hunston & Thompsonin (2000:15) mukaan jotkut sanat ovat merkitykseltään ristiriitaisia. *Byrokraatti*, *opettaja* ja *opiskelija* ovat deskriptiivisiä nimikkeitä, joihin on vaikea yhdistää evaluaatiota. Martin & White (2000), puolestaan ymmärtävät ongelman sekä tunne-, tuominta- että arvostuskuvauksen kategoriaan sopivan sanaston kautta, Ilmaiseeko lause *sepä kiva* tunnetta, arvostusta vai tuomintaa? Evaluaatio on vertailevaa, subjektiivista ja heijastelee viestijän arvojärjestelmää. Hunston & Thompson (2000:22-24) määrittelevät evaluaatiolle neljä parametria, joiden avulla evaluaation tunnistaminen diskurssissa helpottuu.

- ‘Hyvän’ ja 'pahan’ parametri, joka on riippuvainen viestijän arvomaailmasta
- Modaalisuus, joka ilmaisee toteamusten intensiivisyyden tasoa
- Odotettavuuden ja varmuuden taso
- Tärkeyden ja oleellisuuden taso, joka ohjaa yleisöä viestijän tärkeinä pitämien asioiden
  pariin

4.3. Nominalisaatio

Nominalisaatiolla luodaan uuden subjektin lisäksi uusi konsepti, jonka olemassaoloa ei tarvitse perustella. Fairclough (2003: 220) pitää nominalirakenteita "kieliopillisina metaforina", jotka muodostavat toiminnasta subjekteja. Esimerkiksi:

> *”The troops are well trained and prepared. The professionalism and the jointness of the U.S. military will bring us victory.”*

Nominalisaation avulla tiedon määrää ja laatua voidaan rajata ja siihen voidaan sisällyttää evaluaatiota. On oletettavaa, että uhkakuvaukset ottavat ainakin joissakin yhteyksissä nominalisaation muodon, jolla niista luodaan brändejä, joiden olemassaolo on ikäänkuin yleistä tietoa.

Kun tutkitaan esimerkiksi tietoverkkosodankäyntiä käsitteleviä asiakirjoja, voidaan huomata että uhkia on lueteltu eri tavoin, mutta ne tiivistyvät nominalisaatioihin:

> *“According to the 2009 Annual Threat Assessment, ‘‘a successful cyber attack against a major financial service provider could severely impact the national economy, while cyber attacks against physical infrastructure computer systems such as those that control power grids or oil refineries have the potential to disrupt services for hours or weeks’’ and that ‘‘Nation states and criminals target our government and private sector information networks to gain competitive advantage in the commercial sector.”* (Cybersecurity Act 2009)

> *“President Obama said in a speech at Purdue University on July 16, 2008, that ‘‘every American depends—directly or indirectly—on our system of information networks. They are increasingly the backbone of our economy and our infrastructure; our national security and our personal well-being.”* (Cybersecurity Act 2009)

> *“Foreign opponents, through a combination of skill, luck and perseverance, have been able to penetrate poorly protected U.S. computer networks and collect immense quantities of valuable information Although the most sensitive U.S. military communications remain safe, economic competitors and potential military opponents have easy access to military technology, intellectual property of leading companies, and government data. These potential opponents have not hesitated to avail themselves of the opportunities presented by poor cybersecurity.”* (Cybersecurity Act 2009)

Kun on tarpeeksi kuvattu vihollisen toimia sekä itseen kohdistuvia uhkia (tässä myös oman toiminnan kuvauksia), voidaan siirtyä nominalisaatioon, jolla tiivistetään aikaisempia väitteitä ja luodaan mielikuva asioiden nykytilasta:

> *"China's military strategists view the U.S.' dependence on space assets and information technology as its ''soft ribs and strategic weaknesses."* (2008 Report to Congress of the U.S. – China Economic and Security Review Commission)

Kun konsepti on luotu, muut vastaavat ilmaisut eivät enää vaadi selittelyjä:

> *"America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. It is, like Ultra and Enigma, a battle fought mainly in the shadows. It is a battle we are losing."* (Securing Cyberspace for the 44th Presidency)

Konsepti USA:n riippuvuudesta ja haavoittuvuudesta on luotu ja valmis paniikkipolitiikan käytettäväksi. Huomattavaa on se, että nominalisaatio *"America's failure to protect cyberspace"* levisi moniin muihin raportteihin ja lopulta lakialoitteen avauslauseeksi asti, mutta vain yhtenä, tekstistä irrotettuna lauseena. Se summaa lukemattomien raporttien ja uutisten sisällön siitä, mitä kyberrintamalla on viimeisten vuosien aikana tapahtunut. Nominalisaatiot ovat siis uhkakuvien tyypillinen rakenne. Merkittävää niissä on se, että niissä esiintyvän substantiivin pohjana on usein verbi, jota on käytetty diskurssissa aiemmin. Näin toiminnan kuvauksista siirrytään konseptien luomiseen.

4.4. Konstruktivistis-operationaalinen metodi turvallisuustutkimukselle

Buzan, Waever & Wilde (1998) ovat rakentaneet oman viitekehyksen turvallisuusanalyysia varten. Heidän mukaansa turvallisuusanalyysin tavoitteena on selvittää kuka turvallistaa, mitä turvallistetaan (uhat), kenen puolesta, millä tuloksin, ja millaisten ehtojen mukaisesti. Näin ollen analyysimetodi koostuu seuraavista yksiköistä (Buzan, Waever & Wilde, 1998:36):

1. *Referent objects*, eli objektit, joiden olemassaolo kuvataan uhatuksi, ja joiden olemassaolo katsotaan oikeutetuksi.
2. *Securitizing actors*, eli toimijat, jotka turvallistavat asioita ilmaisemalla niiden olemassaolon olevan uhattuna.
3. *Functional actors*, eli vaikuttajat, jotka (objektin ja toimijan lisäksi)

vaikuttavat sektorin dynamiikkaan (esim. asevalmistajat)

Objektit ovat turvallisuusretoriikassa tyypillisesti valtioita ja kansoja. Sodan diskurssissa tyypillistä on myös kansan identiteetin ja arvomaailman asettaminen puolustettavan objektin asemaan. Kuitenkin vain asettamalla vastakkain kaksi kollektiivia (valtion, kansan, sivilisaation), voidaan käydä diskurssia, joka vahvistaa sisäpiiriin kuulumisen tunnetta sekä me-henkeä (Buzan, Waever & de Wilde, 1998:36). Valtion legitimiteettiä ja oikeutta olemassaoloon harvoin kyseenalaistetaan, joten tältäkin kannalta valtio nousee ensisijaiseksi turvallistamisen kohteeksi. Valtio voidaan katsoa oikeutetuksi äärimmäisten keinojen käyttämiseen silloin, kun sen olemassaolo on uhattuna.

Objektit, toimijat ja vaikuttajat ovat helposti löydettävissä kielen rakenteesta systeemis-funktionaalisen viitekehyksen avulla. Sellaisenaan käytettäväksi viitekehys on liian suppea, sillä se jättää itse toiminnan analysoinnin huomiotta. Se kuitenkin tukee SF-teoriaa ja edesauttaa sen soveltamista turvallisuustutkimuksessa. Käyttökelpoiseksi elementiksi nousee turvallistamisen objekti ja viitekehyksen tarjoama tausta sen analysoimiselle.

4.5. Yhteenveto

Tässä luvussa on käsitelty kolme viitekehystä (SF, Appraisal, Konstruktivistis-operationaalinen metodi), joista rakentuu kyberdiskurssin tutkimiseen tarvittavat metodit. Metodit rakentuvat SF-teorian ympärille: Hallidayn funktionaalinen kieliteoria toimii metodien tukirankana, johon Appraisal-teoria tukeutuu.

Koska tutkimuskohteena on turvallisuuskäsitteen muutos, diskurssista toimitaan viittaukset uhkiin. Toisin sanoen dataksi valitaan toiminnan ja olemisen kuvaukset, joilla viitataan Kiinaan tai Kiinan hakkereihin. Toiminnan ja olemisen kuvaukset luokitellaan prosessikuvausten (materiaalinen, behavioraalinen, jne.) sekä niiden sisältämän evaluaation (tunnekuvaukset, arvostus, tuominta) perusteella. Lopulta dataa arvioidaan konstruktivistis-operationaalisen metodin valossa, joka keskittyy uhkakuvien muodostumisen tutkimiseen: täyttääkö diskurssi turvallistamisen tunnusmerkit, ja mikäli täyttää, mikä on turvallistettava objekti? Tämän viitekehyksen avulla on mahdollista käsitellä dataa ja selvittää vastaukset edelleen tarkentuneisiin tutkimuskysymyksiin:

1. Millaisia tekoja ja millaista toimintaa vastapuoli kohdistaa meihin?
2. Mikä/mitä/millainen vastapuoli on?

Näihin kysymyksiin etsitään siis vastausta

- Toiminnan kuvauksilla: millä tavoin virkamiesraportit kuvaavat Kiinan toimintaa? Toiminnan kuvauksia voidaan lähestyä ensin systeemis-funktionaalisen kieliteorian avulla, määrittelemällä prosessien tyypit. Tämän jälkeen niiden sisältämää evaluaatiota voidaan analysoida Appraisal-teorian avulla.
- Olemisen kuvauksilla: millaisia atribuutteja Kiinaan ja kiinalaisiin liitetään? Olemisen kuvauksia voidaan lähestyä samoilla tavoin kuin toiminnan kuvauksia.
- Nominaalirakenteista: millaisilla nominaalirakenteilla uhkia kuvataan? Nominalisaatio usein muodostaa lauseen subjektin (Actor) jonka funktio lauseessa vastaa konstruktivistis-operationaalisen metodin *referent object* –käsitettä. Nominalisaatiot tiivistävät diskurssin uhkakuvat ja niiden atribuutit lauseiden elementeiksi, jotka paljastavat paljon diskurssin sisältämästä evaluaatiosta.

5. ANALYYSI: 2000-LUVUN SOTA

Kun halutaan tutkia turvallisuuskäsityksessä tapahtuneita muutoksia kielen kautta, on ensin selvitettävä kuinka uhkia sanallistetaan. Tässä analyysissä se tehdään lähestymällä kieltä verbianalyysin kautta, eli tekemisen ja olemisen kuvauksia tutkimalla.

USA:n uhkadiskurssissa kyberuhat jakautuvat kolmeen eri päätyyppiin. Tärkein niistä on sotilaallinen uhka:

- *find a new weapon*
- *operate through foreign nations' military or intelligence-gathering operations*
- *have targeted virtual information resources rather than physical infrastructures*
- *developing offensive nuclear, space, and cyber warfare capabilities*
- *has recognized the importance of cyber operations as a tool of warfare*
- *are being trained in cyber operations at Chinese military academies*
- *is aggressively pursuing cyber warfare capabilities*

Toinen uhkien päätyyppi on ns. fyysinen uhka, eli voimaloiden ja muun kriittisen, ihmisten arkielämään ja terveyteen vaikuttavan infrastruktuurisabotaasin mahdollisuus:

- *can attack millions of computers*
- *show interest in using a cyber-based capability to harm the nation's security interests*
- *gain access and view protected data or cause infrastructure components to operate in an irregular manner*
- *attacks on telecommunications devices to corrupt data*
- *disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures*
- *are targeting our information systems and infrastructure for exploitation and potential disruption or destruction*

Kolmas päätyyppi liittyy USA:n asemaan johtavana talousmahtina:

- *stealing or manipulating information contained in various databases*
- *have easy access to military technology, intellectual property of leading companies, and government data*
- *collect immense quantities of valuable information*
- *download critical military technologies and valuable intellectual property*

Kiinalaiset (hallituksen) hakkerit siis kuvataan uhaksi kriittiselle infrastruktuurille, eli yksilölle omassa kodissaan ja päivittäisissä askareissaan, yrityksille talous- ja teknologiavakoilun kautta, sekä koko valtiolle vaanivan täysmittaisen kyberhyökkäyksen muodossa. Käytetyt verbit kertovat nopeasti sen, mitä diskurssilla halutaan viestiä. Seuraavassa kappaleessa käsitellään datan toiminnan kuvaukset.

5.1. Mitä he tekevät, miten he meitä uhkaavat?

5.1.1. Kapasiteetti

Verbien luokittelu ei ole täysin itsestään selvää. Vertaa seuraavia analyyseja:

- *remain completely hidden*

1. vaihtoehto: Judgment (neg): social esteem: capacity (tuominta (neg.): sosiaalinen kunnioitus: kapasiteetti)

On selvää, ettei ole USA:n kannalta edullista, että hakkerit pysyvät piilossa tehdessään hyökkäyksiä. Evaluaatio on siis tyypiltään negatiivista. Salassa toimiminen on kuitenkin osa kybersodankäyntiä, ja jokainen kybersotaa käyvä valtio pyrkii yleensä toimimaan paljastumatta. Voidaan siis sanoa, että kyse on sotilaallisesta kapasiteetista, mikä on Kiinan kannalta edullista ja siten USA:lle uhka.

2. vaihtoehto: Judgment (neg): social sanction: propriety (Tuominta (neg.): sosiaalinen hyväksyntä: kunniallisuus)

Tämä analyysi tuomitsee Kiinan toiminnan moraalittomana. Salassa toimiminen ymmärretään selkärangattomana ja tuomittavana.

Tulkinta riippuu siis sekä kontekstista että tulkitsijasta. Tässä tutkimuksessa oletetaan sekä USA:n että Kiinan käyvän kybersotaa (tiedustelu, vastatiedustelu, informaatio-operaatiot, palvelinhyökkäykset, etc.) monien muiden maiden lailla. Salassa toimiminen on osa sodankäynnin strategiaa, joten siinä onnistuminen on ennemminkin osoitus toimijan kyvykkyydestä kuin moraalista. Sodan konteksti ikään kuin normalisoi toiminnan, mikä siviilimaailmassa on rikollista. Niinpä ensimmäinen analyysivaihtoehto on pätevä.

Entäpä sitten seuraava toiminnan kuvaus:

- disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures

1. vaihtoehto: Judgment (neg): social esteem: capacity (tuominta (neg): sosiaalinen kunnioitus: kapasiteetti)

Tässä tulkinnassa hyökkäys siviili-infrastruktuuria kohtaan pidetään osoituksena sotilaallisesta kapasiteetista, joka on USA:lle uhka, mutta Kiinalle etu. Vaikka tämä aktiivisessa sotatilanteessa olisikin totta ja infrastruktuurin vahingoittaminen osa normaalia, olisi fyysinen siviiliyhteiskunnan lamauttaminen ja ilman aktiivisen sodan kontekstia tuomittavissa sabotaasissa. Niinpä analyysivaihtoehto olisi ennemminkin seuraava:

2. vaihtoehto: Judgment (neg): social sanction: propriety (Tuominta (neg): sosiaalinen hyväksyntä: kunniallisuus)

Toisin sanoen energialaitoksiin ja pankkeihin hyökkääminen ja niiden mahdollinen vahingoittaminen tuomitaan rikolliseksi tai sabotaasiksi.

Yllä kuvatut tulkintaerot ja –vaikeudet ovat sikäli odotettavissa, että tietoverkko-operaatioiden rinnastuminen sodankäyntiin ei ole yksinkertaista. Käytetyt toiminnan kuvaukset kertovat osin sodasta ja osin toisenlaisesta uhasta: *vihollinen hyökkää, operoi, häiritsee, tiedustelee, kehittää* ja *kouluttaa,* mutta myös *varastaa, manipuloi, tunkeutuu* ja *hakkeroi*.

Data paljastui lähestulkoon täysin vastapuolen kapasiteetin kuvailuksi. Samalla ne ovat vahvoja uhkakuvauksia. Seuraavista poiminnat datasta ovat tyyppiesimerkkejä siitä, millä tavoin Kiinan toimintaa kuvataan:

could use	our computer networks to deal us a crippling blow	material, material
[perpetrate	cyberintrusions]	material
gain access and view	protected data or cause infrastructure components to operate in an irregular manner	material, material
stealing or manipulating	information contained in various databases	behavioral, material
continue to develop and field	disruptive military technologies	material
changing	regional military balances	material
have	implications beyond the Asia-Pacific region	relational possessive
has recognized	the importance of cyber operations as a tool of warfare	mental

focusing	[resources and training] on cyber operations	material
can engage	in forms of cyber warfare so sophisticated	material (relational possessive)
enter and disrupt	computer networks	material
are being trained	in cyber operations at Chinese military academies	material
has	"great interest" [in cyber space]	mental
can access	the NIPRNet	material

Tyypillinen toiminnan kuvaus on siis materiaalinen prosessi, eli konkreettista tekemistä ilmaiseva verbi. Ne pyrkivät kertomaan tosiasioista, ja niiden sisältämä evaluaatio korostaa vastapuolen kyvykkyyttä käydä sotaa tietoverkoissa, resursseja sekä koulutusta. On huomattava, että nämä attribuutit ovat juuri niitä, joita mikä tahansa valtio tavoittelee. Vaikka mukana on moraalista tuomintaa sisältäviä toiminnan kuvauksia kuten *varastaa* ja *häiritä*, kuvatun sodan konteksti ikään kuin normalisoi ne kapasiteetin attribuuteiksi. Esimerkiksi:

have been able to penetrate	poorly protected U.S. computer networks	material	Judgment: social esteem: capacity

Tunkeutuminen USA:n tietoverkkoihin voidaan tulkita kontekstista riippuen rikolliseksi tai moraalittomaksi, mutta päällimmäinen viesti on se, että vastapuoli on taitava ja valmis käyttämään taitojaan myös kyseenalaisella tavalla, jos se on sodankäynnillisesti tärkeää.

Pieni mutta retorisesti merkittävä osa toiminnan kuvauksia ovat mentaaliset kuvaukset:

believe	the United States already is carrying out offensive cyber espionage and exploitation against China	mental	Affect: insecurity
believe	that in many cases a vulnerable U.S. system could be unplugged in anticipation of a cyber attack.	mental	Affect: security
believe	the United States is dependent on information	mental	Affect: security

	technology		
believe	there is a first mover advantage in both conventional and cyber operations against the United States	mental	Judgment: social esteem: capacity

Kuten aikaisemmin todettiin, on toisen osapuolen ajatusten kommentoiminen aina vahva kannanotto. Tässä kannanotto korostuu, sillä yllä olevissa kuvauksissa tehdään koko kyberstrategian kannalta oleellinen väite. Ensin kerrotaan Kiinan pitävän kybersotaa ensimmäisenä puolustuskeinona. Lopulta todetaan, että Kiina *uskoo* USA:n jo toteuttavan kybertiedustelua Kiinaa vastaan. Toisin sanoen Kiina *uskoo* kyberiskujen olevan välttämättömiä ja oikeutettuja tälläkin hetkellä. Lisäksi Kiina *uskoo,* että toimimalla nopeasti ja ensimmäisenä se maksimoisi hyödyn heikkojen tietoverkostojen USA:ta vastaan. Tässä argumentissa on käytössä koko datan ainoa kiinalaisten epävarmuutta kuvaava prosessi: se, että Kiina kokee olevansa uhattu, ja voi siis hyökätä milloin vain.

5.1.2. Kunniallisuus

Osapuolen kunniallisuuden evaluointi lienee sotaretoriikan sekä informaatiosodan vanhimpia perinteitä. Tämän tutkimuksen data on sikäli poikkeuksellista, että vastapuolen kunniallisuus ei joudu aggressiivisen demonisoinnin kohteeksi. Toiminnan kuvauksiin liittyy moralisoiva sävy, mutta kyseessä ei ole tyypillinen demonisointiprosessi. Brutaalien hirviöiden sijaan vastapuolesta rakennetaan mielikuvaa salakavalina, taitavina muukalaisina, jotka toimivat USA:ta vastaan, ja ulottavat toimintansa tavallisten ihmisten arkeen. Joskus on ongelmallista erottaa toisistaan kapasiteetin ja kunniallisuuden evaluaatio, sillä se, mikä vastapuolelle on kapasiteettia, esimerkiksi sähköverkon sabotoiminen, voi merkitä ”meille” raukkamaisuutta, rikollisuutta, tai moraalittomuutta. Tässä tutkimuksessa kapasiteetti ja kunniallisuus on erotettu sodankäynnillisyyden perusteella. Hyökkäykset siviili-infrastruktuuria kohtaan ns. rauhan aikana on tulkittu kuvaamaan vihollisen moraalia, kun taas sotilaallisen toiminnan kuvaukset tulkittiin kapasiteetiksi. Seuraavista toiminnan kuvauksista löytyy negatiivismoralistinen sävy:

disrupt	telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures	material
have connections	to terrorist groups	relational possessive
closely monitors	Internet activities	material
are targeting	our information systems and	material

	infrastructure for exploitation and potential disruption or destruction	
have	other terrible things they can do to us	relational possessive

On selvää, että joiltakin osin toiminnankuvaukset voivat olla päällekkäisiä, mutta joissakin niistä moraalinen tuominta on selvemmin näkyvillä.

5.2. Nominaalirakenteet

Nominalisaatiodata täydentää toiminnan kuvauksia ”kieliopillisina metaforina”. Ne sisältävät substantiiviksi muuttuneen verbin:

Nominalisaatio	*Vastapuolen toiminta*
infiltrations into U.S. cyberspace	infiltrate U.S. cyberspace
These investments by China’s military	China invests
China’s developments in these areas	China develops in these areas

Esimerkit havainnollistavat, kuinka nominaalirakenne tiivistää toiminnan ja brändää sen konseptiksi. Vaikka tässä tutkimuksessa toiminnan kuvausten tutkiminen rajoitetaan ns. viholliskuvauksiin, on nominaalidataan sisällytetty myös ns. itseen viittaavat rakenteet. Alla dataan on sovellettu samaa evaluaatioanalyysiä kuin jo käsiteltyihin toiminnan kuvauksiin:

ME ITSE	the adequacy of existing legal authorities	Judgment: social esteem: capacity
	the incapacity or destruction of such systems and assets	Judgment: social esteem: capacity
	the vulnerability of U.S. infrastructures	Judgment: social esteem: capacity
	Our lack of cybersecurity	Judgment: social esteem: capacity
VASTAPUOLI	China’s developments in these areas	Judgment: social esteem: capacity
	the natural progression of those wishing to harm U.S. security interests	Judgment: social sanction: propriety
	violent extremism in support of a radically different worldview	Judgment: social sanction: propriety
	the emergence of powerful new state competitors	Judgment: social esteem: capacity

“Itseen” viittaavat nominaalirakenteet kertovat siis kapasiteetin puutteesta, kun taas vastapuoleen viittaavat rakenteet koostuvat heidän kapasiteettinsa muodostamasta uhkasta, sekä muutamissa tapauksissa moraalin evaluoinnista.

Nominaalirakenteet tiivistävät uhkakuvat lähes parhaiten. Niihin on valikoitunut kannanottoja, jotka tiivistävät kyberdiskurssissa käytetyt

toiminnan kuvaukset niin, että vain niitä vilkaisemalla voi nähdä minkä asioiden pariin diskurssi keskittyy: vastapuolen *kehitykseen* ja heidän suorittamiinsa *tunkeutumisiin* ja *hyökkäyksiin*, sekä omaan *haavoittuvuuteen* ja *puutteisiin*.

6. JOHTOPÄÄTÖKSET

6.1. Asevarustelukilpaa ja tietokilpailua

> *"Wartime propaganda is effective only when linked to a national policy that it can exploit and with which the masses can identify. It is for this reason that the 9/11 attacks were packaged as our generation's Pearl Harbor."*
> (Huhtinen & Rantapelkonen, 2009:39)

Kuten terrorismi siviileihin kohdistuvine hyökkäyksineen, myös tietoverkkohyökkäykset tarjoavat yhteiskunnalle uuden pelonaiheen. Siinä missä *terrorismi* edusti pahuuden, taantumuksen ja vierauden pelkoa, *cyber* tarkoittaa teknologiaa ja edistyksellisyyttä – kaikkea sitä, mitä länsimaiseen kulttuuriin on totuttu yhdistämään. Kysymys onkin siitä, kuinka paljon uhkaa me siedämme? (Ventre, 2009) Tähän pelkoon on helppo tarttua, varsinkin jos motiivina on siitä hyötyminen poliittisesti. Syyskuun terrori-iskujen jälkeen pelättiin uutta hyökkäystä ydinvoimaloihin ja muihin kriittisen infrastruktuurin kohteisiin. Nyt sitä pelätään taas. Modernit uhat ovat samanlaisia niin sotilaille kuin siviileillekin. Ventre summaa asian toteamalla, että ”uhka” käyttää hyväkseen ”heikkoutta”. Jos tunnemme olomme uhatuksi, on meillä myös tunne omasta heikkoudestamme. ”Eikö kiinalainen uhka ruoki uudenlaista paranoiaa amerikkalaisessa yhteiskunnassa? (2009)”

Kyberdiskurssia tarkasteltaessa huomio kiinnittyy ensin vertauksiin. Kyberdiskurssi ei tällä hetkellä ole perinteistä sotaretoriikkaa. Vihollinen ei ole demonisoinnin kohde, eikä omaa toimintaa yritetä puolustella glorifioimalla. Sen sijaan että omista tappioista vaiettaisiin, niitä korostetaan, dramatisoidaan, ja niistä kerrotaan yksityiskohtaisia tarinoita joita höystetään asiaa konkretisoivilla vertauksilla. USA:n virkamiehistö rakentaa kuvaa taantuvasta sotilasmahdista, joka on ennen kaikkea uhri ja vaarassa. Kyberdiskurssissa ei ole sankareita. Vihollinen on kasvoton mutta taitava ja tehokas, ja pystyy käymään ikään kuin miehittämätöntä sotaa USA:n kustannuksella. Vastapuoli ei ole epäinhimillinen ja moraaliton paha, vaan laskelmoiva ja epäluotettava asiantuntija – vastakohta sille, millaiseksi esimerkiksi irakilaisviholliset on kuvattu. Se millaiseksi kiinalaista kybersotilasta luonnehditaan, on ennemminkin kateuden aihe. Onhan tehtävänsä kylmän rauhallisesti ja taitavan huomaamattomasti suorittava, maalleen lojaali sotilas juuri sitä, mitä jokainen armeija tarvitsee. Toisaalta tekojaan peittelevä, epäluotettava vastapuoli on aina uhka ja demonisoitu (Ventre, 2009).

Tietoverkkosodankäynnin tuomat uhkakuvat ja turvallisuuskäsitykset liittyvät pääasiassa modernisoituvan Kiinan teknologiseen ja inhimilliseen

kapasiteettiin ja resursseihin, mutta myös arkielämään ja yhteiskunnan infrastruktuuriin, sekä Yhdysvaltojen asemaan johtavana talousmahtina. Kiina vaurastuu, ja Yhdysvallat kamppailee pitääkseen yritykset kotimaassa. Vakoilua pelätään niin sotilas- kuin yritysmaailmassa. Kiinalaiset ja intialaiset insinööriopiskelijat ovat tuttu näky länsimaisissa yliopistoissa. Yhdysvallat on jälleen mukana kylmän sodan kilvassa:

> *"Similar to the period after the launch of the Sputnik satellite in October, 1957, the United States is in a global race that depends on mathematics and science skills. According to a report published by The Economist, talented information technology (IT) employees "are already in short supply everywhere, but the situation will get tougher, as the nature of skills needed is changing. In addition to technical knowledge, tomorrow's IT employee will require expertise in project management, change management and business analysis."*(Cyberspace Policy Review, 2009)

Kyse on jälleen siitä, kuka keksii ensin tehokkaan aseen, tällä kertaa kyberavaruudessa, ja kuka ensin löytää sille tehokkaan vastakeinon. Puolustus on kallista ja vaikeaa, eikä informaatioavaruutta voida kontrolloida tai turvata (Ventre, 2009). Diskurssissa ollaan nyt etenemässä keskusteluun siitä, millä tavalla tietoverkkohyökkäykset voitaisiin sisällyttää länsimaisen sivistysvaltion doktriiniin. Keskustelu arjen valintojen vaikutuksesta jää pahasti suureellisen diskurssin varjoon. Puhutaan kansalaisten kouluttamisesta ja riskitietoisuuden lisäämisestä (Cyberspace Policy Review, 2009), mutta pitkän linjan ratkaisuiksi tarjotaan vain lisärahoitusta, tietoverkkosodankäyntiin erikoistuneen henkilöstön koulutusta ja internet-rajoituksia.

On selvää, että kyberdiskurssi ja turvallisuuspoliittisen diskurssin todellisuus ovat kaksi eri asiaa. Niin kuin terrorisminvastainen sotakin, tietoverkkosodankäynti on myös pitkälti informaatiosotaa ja retoriikkaa. Kuten Bendraft (2004) totesi, kyberdiskurssissa on kyse ennemminkin salaisista agendoista kuin turvallisuuden luomisesta.

6.2. Kyberdiskurssi 2000-luvun lopussa

Kun käsite "terrorisminvastainen sota" presidentti Obaman toiveesta keväällä 2009 haudattiin, kyseessä oli suuri retorinen muutos. Terrorisminvastainen sota ei tietenkään kadonnut mihinkään – päinvastoin, Afganistanissa joukkoja ollaan vuoden 2009 loppuun mennessä vain lisäämässä. Terrorismin vastainen sota haluttiin kuitenkin pois diskurssin keskiöstä. Paluu roistovaltioiden ja muiden valtiollisten

uhkien määrittelyyn merkitsee paluuta kylmän sodan retoriikkaan, josta teknologinen kilpajuoksu on vain yksi esimerkki. Retoriikassa kyberuhat on luontevasti nostettu ydinaseuhan ja perinteisen sodankäynnin rinnalle. Tietoverkkohyökkäyksen vaikutuksia kuvataan samoilla mielikuvilla kuin ohjus- tai terrori-iskun vaikutuksia.

Tietoverkkosodankäynti on uusi taistelumuoto, joka selvästi hakee paikkaansa suurvaltojen doktriineissa. Yhdysvalloissa tilanne on erikoinen sikäli, ettei sen johtoasema yhtäkkiä olekaan itsestään selvä. Teknologian johtomaa pelkää tietovuotoja ja resurssien riittämättömyyttä.

Tässä epäsymmetrisessä sodassa taloudellinen vauraus ei takaa automaattista etulyöntiasemaa, sillä Yhdysvalloilla on vastassaan taloudellisessa nousussa oleva autoritäärinen valtio, joka voi kohdistaa resurssinsa haluamallaan tavalla, ilman kädenvääntöä kansan yleisen mielipiteen kanssa.

Tämä tutkimus on ollut paitsi tutkimus uhkakuvista, myös mediaseurantaa turvallistamisprosessin kulusta. Yhdysvalloissa ratkaisuksi uhkiin on tarjottu paitsi rajoituksia, myös tietoverkkoinfrastruktuurin valtiollistamista:

> *”The White House must lead the way forward. The Nation’s approach to cybersecurity over the past 15 years has failed to keep pace with the threat. We need to demonstrate abroad and at home that the United States takes cybersecurity-related issues, policies, and activities seriously. This requires White House leadership that draws upon the strength, advice, and ideas of the entire Nation.”*
> (Cyberspace Policy Review, 2009)

Uhan tullessa alueelta jota hallitus ei voi kontrolloida, on luonnollista että valtio pyrkii kasvattamaan valtaansa ja lunastamaan päävastuun turvallisuuskeskustelussa. Yhdysvalloissa käydäänkin eräänlaista kahden rintaman sotaa: yhtäällä suojaudutaan tietoverkkohyökkäyksiltä ja tehdään toimintasuunnitelmaa omaa toimintaa varten, ja toisaalla toteutetaan informaatio-operaatiota, jonka tavoitteena tarvittavan poliittisen vallan saavuttaminen ja sitä kautta toimintamahdollisuuksien kasvattaminen kotimaassa. Kyberdiskurssia voidaan tarkastella propagandan sääntöjen valossa (Huhtinen, 2005: 151):

- *Ensimmäinen sääntö propagandan onnistumiselle on, että haluttua teemaa tulee toistaa mahdollisimman usein ja mahdollisimman monia vaikutuskanavia hyväksikäyttäen.*

Kyberuhat ovat olleet esillä eri medioissa. Vuoden 2005 jälkeen virkamiesraportteja sekä akateemisia tutkimuksia on julkaistu runsaasti. Media on tarttunut niihin halukkaasti, ja suurimpia tutkimuksia on seurannut aina pitkä seurantakausi eri medioissa. Esimerkiksi *Ghostnet*-raportin uutisointi nosti pinnalle Pentagoniin kohdistuneet hyökkäykset edellisvuosilta, ja uusista hyökkäyksistä (tai niiden yrityksistä) uutisoitiin lähes päivittäin. Aktiivinen uutisointi puolestaan vaikuttaa valtakunnan poliittiseen siipeen, ja synnyttää tarpeen uusille tutkimuksille.

- *Propagandan toinen pääsääntö on se, että siinä on löydettävä oikea sävy. Tämä edellyttää kohdekult-tuurin sisärakenteiden, merkitysjärjestelmien ja tunnetilojen tuntemusta.*

Hyvä esimerkki tunnetilojen tuntemuksesta on mm. terrorismin käyttäminen villinä korttina. Vaikka terrorisminvastainen sota onkin virallisesti käsitteenä haudattu, voidaan terroriuhkaan aina tarvittaessa palata. Seuraava *Ghostnet*-raporttia puiva Wall Street Journalin (9.4.2009) artikkeli kiteyttää amerikkalaisen terrori-trauman:

> *“Sen. Charles Schumer said he was alarmed by the report and was throwing his support behind a measure to create a White house cybersecurity adviser and augment the federal role in bolstering the country’s cyberdefenses. ”Today it is China and Russia, but the same tools are potentially available to Iran and al Qaeda and others who may actively seek to do us harm[.]”*

Terrori-iskun aiheuttama traumaa ei voi vähätellä, eikä se koske ainoastaan amerikkalaisia. Toinen taitavasti hyödynnetty arvo ja tunnetila on amerikkalainen tottumus ajatella Yhdysvaltoja teknologisena edelläkävijänä ja maantieteellisesti eristäytyneenä suurvaltana. Nyt vihollinen kuvataan teknologiseen ylilyöntiasemaan, amerikkalaiset heikoiksi, voimattomiksi, ja vastapuolen ulottuvilla oleviksi. Pelko aktivoi ihmiset, ja paniikkipolitiikalle on jälleen tilausta.

- *Kolmas propagandan sääntö on, että asia pitää kiteyttää helposti omaksuttavaan iskulausemuotoon.*

Tähtien sota -brändi on palaamassa sotanäyttämölle (Huhtinen & Rantapelkonen, 2007). Kybersotaa ollaan viemässä kylmän sodan suuntaan, ja se näkyy myös sen diskurssista. Kun tarkastellaan tämän tutkimuksen kielitieteellistä todistusaineistoa, voi tulevasta brändistä päätellä jo jotakin:

- *increasing cyber-intrusions*
- *the high-profile attacks and more routine infiltrations*
- *the increasing pace and volume of cyber intrusions*
- *infiltrations into U.S. cyberspace*
- *China's current cyber operations capability*
- *and the spread of technologies*
- *growing connectivity*

Kybersodan brändiä leimaa nopeus ja informaatio. Kansalaisia mobilisoiva pelkoheräte ja iskulause sen sijaan sisältää viitteet haavoittuvuuteen, epäonnistumiseen ja puutteisiin:

- *the vulnerability of U.S. infrastructures*
- *America's failure to protect cyberspace*
- *Our lack of cybersecurity*

Toimimatta jättäminen ei ole vaihtoehto. Nähtäväksi jää, tapahtuuko tässä retoriikassa muutos perinteisempään suuntaan, jossa vastustaja haastetaan avoimesti, ja omasta suorituskyvystä puhutaan luottavaisesti sekä sisä- että ulkopolitiikassa.

6.3. Kyberdiskurssin tavoitteet ja lingvistiset johtolangat

Terrorisminvastaisen sodan käsitteen painaminen taka-alalle ja valtiokeskeisten uhkakuvien nostaminen diskurssin keskiöön voi merkitä lukemattomia asioita. Kiinan vaurastuminen ja asevoimien modernisointi tiedetään haasteeksi Yhdysvaltojen ulkopolitiikalle. Kiinalla on resursseja, joita ei-valtiollisilla ryhmittymillä ei ole. Juuri resurssien tarve ajaa retoriikkaa kohti Kylmän Sodan perinteitä.

Silmäys eri tietoverkkojen turvallisuutta käsitteleviin raportteihin paljastaa suosituimmaksi turvallisuuden parannusehdotukseksi lisärahoituksen. Listalla ovat myös koulutus, sekä erilaiset byrokraattiset uudelleenjärjestelyt valtiohallinnon ja asevoimien sisällä. Diskurssissa perustellaan valtion olevan ainoa vaihtoehto päävastuun kantajaksi. Valtion väliintulolla lienee myös protektionistinen motiivi, sillä Kiina-ilmiö uhkaa viedä IT-teollisuuden pois Yhdysvalloista. Tärkein syy internet-infrastruktuurin ja verkkoturvallisuuden valtiollistamiselle on kuitenkin vallan ja valvonnan laajentaminen kyberavaruudessa.

Diskurssianalyysi paljasti Yhdysvaltojen olevan jatkuvasti ei-toivotun, vaaralliseksi kuvatun toiminnan kohteena. Irak-retoriikassa toiminnan kohteeksi joutumista kuvattiin yleensä silloin, kun tarvittiin perusteita

omalle toiminnalle. Hyökkäys laillistaa puolustuksen, vaikka se toteutettaisiin ennaltaehkäisevänä hyökkäyksenä.

> *”Hälyttävää on myös se, että DoD:lla ei ole doktriiniperustaa tietoverkkosodankäynnille. Olemassa olevat doktriinit ja säännöt kohdistuvat kansalliseen tietoturvaan ja verkkoturvallisuuteen, mutta eivät itse tietoverkkosodan-käyntiin.”* (Viestimies, 2/2009)

On oletettavaa, että kyberdiskurssi tähtääkin offensiivisen tietoverkkosodankäynnin integroimiseen Yhdysvaltain asearsenaaliin. Vastapuolen toiminnan kuvaukset toimivat tässä yhteydessä legitimoivana argumenttina. Diskurssissa ei myöskään ole unohdettu mainita Kiinan doktriinia, joka Yhdysvaltojen mukaan perustuu *first-mover advantage* -periaatteelle.

Diskurssin tavoitteista kertoo myös arkisempien suoja- ja turvatoimenpiteiden pyyhkäiseminen sivuun. Keskustelu sivuuttaa esimerkiksi tavoitteet infrastruktuurin nopean toipumisen varmistamisesta.

Pääosaa tässä tutkimuksessa näyttelivät tekemisen ja olemisen kuvaukset, eli verbit. Uhkakuviksi koetaan nimenomaan vastapuolen toimet sekä oma tekemättömyys ja passiivisuus. Näin ollen tekemisen kuvausten luokittelu ja analysointi oli toimiva tapa lähestyä uhkadiskurssia. Toiminta, tekeminen ja aktiivisuus ovat paitsi sodankäynnin, myös länsimaisen arvomaailman perusta. Näin ollen se on myös sotaretoriikan ydin.

LÄHTEET

Bendrath, Ralf. (2003). The American Cyber-Angst and the Real World - Any Link?. Teoksessa Latham, R. (Ed.) 2003. *Bombs and Bandwidth: The emerging relationship between information technology and security.* The New Press, New York.

Butt, David G., Lukin, Annabelle, and Matthiessen, Christian M.I.M. 2004. "Grammar: the first covert operation of war." *Discourse and Society 15* (2-3): 267-290.

Buzan, B., Waever, O., and De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers, London.

China Economic and Security Review Commission (2008). 2008 Report to Congress. Washington: U.S. Government printing Office, 2008.

CSIS. Center for Strategic and International Studies (2008). Securing Cyberspace for the 44th Presidency. Washinton, DC, 2008.

Fairclough, Norman (2003). *Analyzing discourse: Textual analysis for social research.* Routledge, London.

Fallows, James (2009). "Civilize Homeland Security." The Atlantic Jul/Aug 2009. November 30, 2009. <http://www.theatlantic.com/doc/200907/ideas-homeland-security>.

van Dijk, Teun A. (1995). "Ideological discourse analysis." *The New Courant, 4/1995: Interdisciplinary Approaches to Discourse Analysis*. 135-61. Ed. Ventola, E. & Solin, A. Helsinki University Press: Helsinki.

Granick, Jennifer (2009)."Federal Authority Over the Internet? The Cybersecurity Act of 2009." Electronic Frontier Foundation. April 10, 2009. November 30, 2009. <http://www.eff.org/deeplinks/2009/04/cybersecurity-act>

Haddington, Pentti. (2005). *The intersubjectivity of stance taking in talk-in-interaction*. Doctoral dissertation. P. Haddington, Oulu.

Halliday, M.A.K. (2004). *An introduction to functional grammar*. 3rd edition. Revised by M.I.M. Mathiessen. Arnold, London.

Hayes, B. (2009). *Neoconopticon: The EU Security-Industrial complex.* Transnational Institute.

Huhtinen, A-M. (2005). *Sanasota: Johdatus sodan ja sodanjohtamisen filosofiaan*. Toim. Tuomo Aimonen. Elan Vital, Helsinki.

Huhtinen A-M. & Rantapelkonen, J. (2007). *Messy Wars.* Finn Lectura, Tampere.

Huhtinen, A-M. & Rantapelkonen, J. (2009). *Bumerangi: 69 blogia turvallisuudesta*. Elan Vital, Helsinki.

Hunston, S. & Thompson, G. (ed.) (2000). *Evaluation in text authorial stance and the construction of discourse.* Oxford University Press, Oxford.

Kuparinen, V-P. (2009). Johtaja. Huoltovarmuuskeskus, infrastruktuuriosasto. Haastattelu. 25.8.2009.

Kärkkäinen, A. (2009). "Tietoverkkosodankäynti sotilaallisena suoritus-kykynä." *Viestimies* 2/2009.

Lewis, J.A. (2007). "There's No Such Thing As Cyberterror." Atlantic Community. 25 July 2007. 30 November 2009. <http://www.atlantic-community.org/index/Open_Think_ Tank _Article/There%27s_ No_Such_Thing_As_Cyberterror>.

Martin, J.R. and White, P.R.R. (2005). *The language of evaluation: Appraisal in English*. Palgrave Macmillan, New York.

Owen, W.A., Dam, K. W., & Lin, H.S. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Computer Science and Telecommunications Board. The National Academies Press, Washington.

Paldanius, H. (2005). "Information and messages in Finland's threat scenarios." *Struggling toUnderstand Information War*. Ed. Kuusisto, R. & Rantapelkonen, J. Hakapaino, Helsinki.

Pulkkinen, A. (2004). "Pysyvän poikkeustilan politiikka. Sodan oikeutuksen narratiivi Yhdysvaltain globaalin maailmanvallan vahvistajana." *Kosmopolis 2/2004*. 33-49.

Schneier, Bruce (2009). "Who Should Be in Charge of Cybersecurity?" The Wall Street Journal. March 31, 2009. November 30, 2009. <http://online.wsj.com/article/SB12384457975337 0907.html>.

Tuohinen, Petteri (2009). "Yhdysvalloilla ja Kiinalla riitasointuja nyt kaikilla rintamilla." Helsingin Sanomat 20 syyskuuta, 2009.

Ventre, Daniel. (2009). *Information Warfare.* ISTE, London.

Yhdysvallat. Pentagon (2007). Speech as delivered by Deputy Secretary of Defense Gordon R. England. Falls Church, VA, October 05, 2007. <http://www.defense.gov/Speeches/Speech. aspx?SpeechID=1317>

Yhdysvallat. Pentagon (2008). Speech as delivered by Secretary of defense Rbert M. Gates. Washington, D.C., October 28, 2008. <http://www.defense.gov/speeches/speech.aspx?speechid =1305>

Yhdysvallat. S 773 IS (The Cybersecurity Act of 2009). Lakialoite. Washington, DC, 2009.

Yhdysvallat. White House (2009). Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Comunications Infrastructure. Washington, 2009.

Yould, R. (2003) ” Beyond the American Fortress: Understanding Homeland Security in the Information Age”. Teoksessa Latham, R. (Ed.) 2003. *Bombs and Bandwidth: The emerging relationship between information technology and security.* The New Press, New York.

Zizek, Slavoj. (2009). *Violence*. Profile Books, London.

Liite 1. Tekemisen ja olemisen kuvaukset

Action	*Complement*	*Process type*	*Appraisal*	(explanation for choice)
find	a new weapon	material	Judgment: social esteem: capacity (neg)	increasing their power
can attack	millions of computers	material	Judgment: social esteem: capacity (neg)	increasing their power
infect	hundreds of thousands	material	Judgment: social esteem: capacity (neg)	increasing their power
remain	completely hidden	relational attributive	Judgment: social esteem: capacity (neg)	experienced, guerilla-like
could use	our computer networks to deal us a crippling blow	material, material	Judgment: social esteem: capacity (neg)	know how to take advantage
have been quick to recognize	the [rise of cyber-espionage]	mental	Judgment: social esteem: capacity (neg)	up to date, educated
[perpetrate	cyberintrusions]	material	Judgment: social esteem: capacity (neg)	conduct sophisticated warfare
operate	through foreign nations' military or intelligence-gathering operations	material	Judgment: social esteem: capacity (neg)	take advantage of weaknesses
have connections	to terrorist groups	relational possessive	Judgment: social sanction: propriety	immoral
operate	as individuals	material	Judgment: social esteem: capacity (neg)	hard to trace, guerilla-like
wish to steal or manipulate	protected data on secure federal systems	mental	Judgment: social sanction: propriety	expert, unreliable
[successfully infiltrate]		material	Judgment: social esteem: capacity (neg)	clever, expert
have been working	in coordination with foreign military organizations or (foreign) state intelligence services	material	Judgment: social esteem: capacity (neg)	expert, increasing their military capacity
show interest	in using a cyber-based capability to harm the nation's security interests	behavioral, behavioral	Judgment: social sanction: propriety	harm civilians

Action	*Complement*	*Process type*	*Appraisal*	(explanation for choice)
gain access and view	protected data or cause infrastructure components to operate in an irregular manner	material, material	Judgment: social esteem: capacity (neg)	expert, waging cyberwar
stealing or manipulating	information contained in various databases	behavioral, material	Judgment: social esteem: capacity	expert, waging cyberwar
attacks	on telecommunications devices to corrupt data	material, material	Judgment: social sanction: propriety	harm civilians
cause infrastructure components to operate	in an irregular manner	material	Judgment: social esteem: capacity	expert, waging cyberwar
have targeted	virtual information resources rather than physical infrastructures	material	Judgment: social esteem: capacity (neg)	expert, waging cyberwar
will transition	from stealing or manipulating data to undertaking action that temporarily or permanently disables or destroys the telecommunication network or affects infrastructure components	material, behavioral material, material, material, material, material	Judgment: social sanction: propriety Judgment: social esteem: capacity (neg)	expert, waging cyberwar
disrupt	telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures	material	Judgment: social sanction: propriety	harm civilians
have	the potential to disrupt services for hours to weeks	relational possessive, material	Judgment: social esteem: capacity (neg)	expert, waging cyberwar
are targeting	our information systems and infrastructure for exploitation and potential disruption or destruction	material	Judgment: social sanction: propriety	expert, waging cyberwar
have	other terrible things they can do to us	relational possessive	Judgment: social sanction: propriety	harm civilians

Action	*Complement*	*Process type*	*Appraisal*	(explanation for choice)
are working on	harder	material	Judgment: social esteem: tenacity (neg)	hard-working
are	better able to do	relational attributive	Judgment: social esteem: capacity	expert
seem to be	more motivated to do	relational attributive	Judgment: social esteem: tenacity (neg)	hard-working
continue to develop and field	disruptive military technologies	material	Judgment: social esteem: capacity (neg)	increasing their military capacity
changing	regional military balances	material	Judgment: social esteem: capacity (neg)	increasing their power
have	implications beyond the Asia-Pacific region	relational possessive	Judgment: social esteem: capacity (neg)	increasing their power
developing	offensive nuclear, space, and cyber warfare capabilities	material	Judgment: social esteem: capacity (neg)	increasing their military capacity
have	the potential to be truly global	relational possessive	Judgment: social esteem: capacity (neg)	increasing their power
is devoting	a great deal of attention and resources to developing outer space and cyber space capabilities	material	Judgment: social esteem: capacity (neg)	increasing their military capacity
view	the U.S.' dependence on space assets and information technology as its ''soft ribs and strategic weaknesses.''	mental	Judgment: social esteem: propriety	take advantage of weaknesses
are	significant	relational attributive	Judgmen: social esteem: tenacity	increasing their power
have affected	other nations	material	Judgment: social esteem: capacity (neg)	increasing their power
has recognized	the importance of cyber operations as a tool of warfare	mental	Judgment: social esteem: capacity (neg)	expert
focusing	[resources and training] on cyber operations	material	Judgment: social esteem: capacity (neg)	increasing their military capacity

Action	*Complement*	*Process type*	*Appraisal*	(explanation for choice)
addresses	both cyber attacks and cyber intrusions	verbal	Judgment: social esteem: capacity (neg)	increasing their military capacity
has	the intent and capability to conduct cyber operations anywhere in the world at anytime	relational possessive, material	Judgment: social esteem: capacity (neg)	increasing their military capacity
has	an active cyber espionage program	relational possessive	Judgment: social esteem: capacity (neg)	espionage is part of warfare
[has	an advanced cyber operations capability]	relational possessive	Judgment: social esteem: capacity (neg)	advanced and capable
can engage	in forms of cyber warfare so sophisticated	material (relational possessive)	Judgment: social esteem: capacity (neg)	expert, capable
[tolerate and maybe even encourage	250 hacker groups]	behavioral	Judgment: social sanction: propriety	hackers vs. military, on the other hand the US has hired hackers as well
enter and disrupt	computer networks	material	Judgment: social esteem: capacity (neg)	expert, waging cyberwar
closely monitors	Internet activities	material	Judgment: social sanction: propriety	regulates liberties, allows cybercrime
is likely aware	of the hackers' activities	mental	Judgment: social sanction: propriety	allows cybercrime
devotes	a tremendous amount of human resources to cyber activity	material	Judgment: social esteem: capacity (neg)	increasing their military capacity
are being trained	in cyber operations at Chinese military academies	material	Judgment: socal esteem: capacity	educated, expert
has	"great interest" [in cyber space]	mental	Judgment: social esteem: capacity	up to date, educated
can access	the NIPRNet	material	Judgment: social esteem: capacity	capable, expert
views	it as a significant Achilles' heel and as an important target of asymmetric capability	mental	Judgment: social sanction: veracity	abusive, unreliable

Action	*Complement*	*Process type*	*Appraisal*	(explanation for choice)
has observed	how the U.S. military has operated successfully overseas	material	Judgment: social esteem: capacity	educated, up to date
has noted	that the United States in many cases utilizes a deployment or buildup phase	mental	Judgment: social esteem: capacity	educated, up to date
is depending	on this	behavioral	Judgment: social esteem: capacity (neg)	dependant
believes	that, by cyber attacking U.S. logistics functions[...] it can delay or disrupt U.S. Forces moving to the theater	mental	Judgment: social sanction: veracity	abusive, unreliable
views	Taiwan's will to fight as the key to success	mental	Judgment: social esteem: capacity	learned, knowledgeable
postulate	that successfully delaying a U.S. response after a hard and fast strike against Taiwan will create a window of opportunity in which it may be possible to force Taiwan to capitulate	mental	Judgment: social sanction: veracity	deceptive
believe	the United States already is carrying out offensive cyber espionage and exploitation against China	mental	Affect: insecurity	fears being targeted
believe	that in many cases a vulnerable U.S. system could be unplugged in anticipation of a cyber attack.	mental	Affect: security	confident with their capability
believe	the United States is dependent on information technology	mental	Affect: security	confident in their position

Action	*Complement*	*Process type*	*Appraisal*	(explanation for choice)
believe	there is a first mover advantage in both conventional and cyber operations against the United States	mental	Judgment: social esteem: capacity	know strategy
is likely to take advantage	of the U.S. dependence on cyber space	behavioral	Judgment: social sanction: veracity	decepive
is aggressively pursuing	cyber warfare capabilities	material	Judgment: social esteem: capacity	have potential and capabilities
have been able to penetrate	poorly protected U.S. computer networks	material	Judgment: social esteem: capacity	increasing their military capacity
collect	immense quantities of valuable information	material	Judgment: social esteem: capacity	increasing their military capacity
have	easy access to military technology, intellectual property of leading companies, and government data	relational possessive	Judgment: social esteem: capacity	increasing their military capacity
have not hesitated to avail	themselves of the opportunities presented by poor cybersecurity	behavioral	Judgment: social sanction: veracity	abusive, unreliable
[intrude]		material	Judgment: social sanction: propriety	harm US society illegally
[hack]		material	Judgment: social sanction: propriety	harm US society illegally
[probe]		material	Judgment: social sanction: propriety	harm US society illegally
are	sophisticated, well resourced and persistent	relational identifying	Judgment: social esteem: capacity	expert
remotely access and download	critical military technologies and valuable intellectual property	material	Judgment: social esteem: capacity	expert
increasing	their cyber-warfare capabilities	material	Judgment: social esteem: capacity	increasing their military capacity

Liite 2. Nominalisaatiot uhkakuvissa: toiminnan kuvauksista johdetut substantiivit ja luodut ”konseptit”

Nominalization	*Appraisal values*
Nominalizations that refer to THEM	
increasing cyber-intrusions into government computer networks	Judgment: social sanction: propriety
the high-profile attacks and more routine infiltrations	Judgment: social esteem: capacity
the natural progression of those wishing to harm U.S. security interests	Judgment: social sanction: propriety
the increasing pace and volume of cyber intrusions	Judgment: social esteem: capacity
infiltrations into U.S. cyberspace	Judgment: social esteem: capacity
The increased resources and training	Judgment: social esteem: capacity
terrorists’ use of technology to degrade the nations infrastructure	Judgment: social sanction: propriety
unauthorized intrusion	Judgment: social sanction: propriety
These investments by China’s military	Judgment: social esteem: capacity
China’s developments in these areas	Judgment: social esteem: capacity
China’s current cyber operations capability	Judgment: social esteem: capacity
violent extremism in support of a radically different worldview	Judgment: social sanction: propriety
the emergence of powerful new state competitors	Judgment: social esteem: capacity
the growth of "walled gardens"	Judgment: social esteem: capacity
Nominalizations that refer to US	
the adequacy of existing legal authorities	Judgment: social esteem: capacity
the incapacity or destruction of such systems and assets	Judgment: social esteem: capacity
the vulnerability of U.S. infrastructures	Judgment: social esteem: capacity
a multi-faceted, technologically based vulnerability	Judgment: social esteem: capacity
America’s failure to protect cyberspace	Judgment: social esteem: capacity
loss of information	Judgment: social esteem: capacity
Our difficulty in coping with new kinds of threats	Judgment: social esteem: capacity
Our lack of cybersecurity	Judgment: social esteem: capacity
the organization of the federal government	Judgment: social esteem: capacity
our failure to defend cyberspace	Judgment: social esteem: capacity
the lack of a defined career path	Judgment: social esteem: capacity
the lack of a public strategy and military doctrine	Judgment: social esteem: capacity
the inconsistencies in applying the old laws to a new paradigm	Judgment: social esteem: capacity
Other nominalizations	
Growing connectivity between information systems, the Internet, and other infrastructures	Judgment: social esteem: tenacity
the global interdependence of economies and network	Judgment: social esteem: tenacity
and the spread of technologies that provide military advantage, which in an earlier time were available only to nation-states	Judgment: social esteem: capacity

Aikaisemmin tässä sarjassa on julkaistu

No 1, 2009
Laaksonen, Marko (2009) *Merkillinen strategia – Puolustushallinnon strategian semioottinen tarkastelu* [Akateeminen väitöskirja]. Edita Prima Oy: Helsinki.

No 2, 2009
Kuokkanen, Pertti (2009) *Communicative and Anticipatory Decision-making Supported by Bayesian Networks* [Akateeminen väitöskirja]. Edita Prima Oy: Helsinki.

No 3, 2009
Toiskallio, Jarmo & Mäkinen, Juha (2009) *Sotilaspedagogiikka: Sotiluuden ja toimintakyvyn teoriaa & käytäntöä*. Edita Prima Oy: Helsinki.