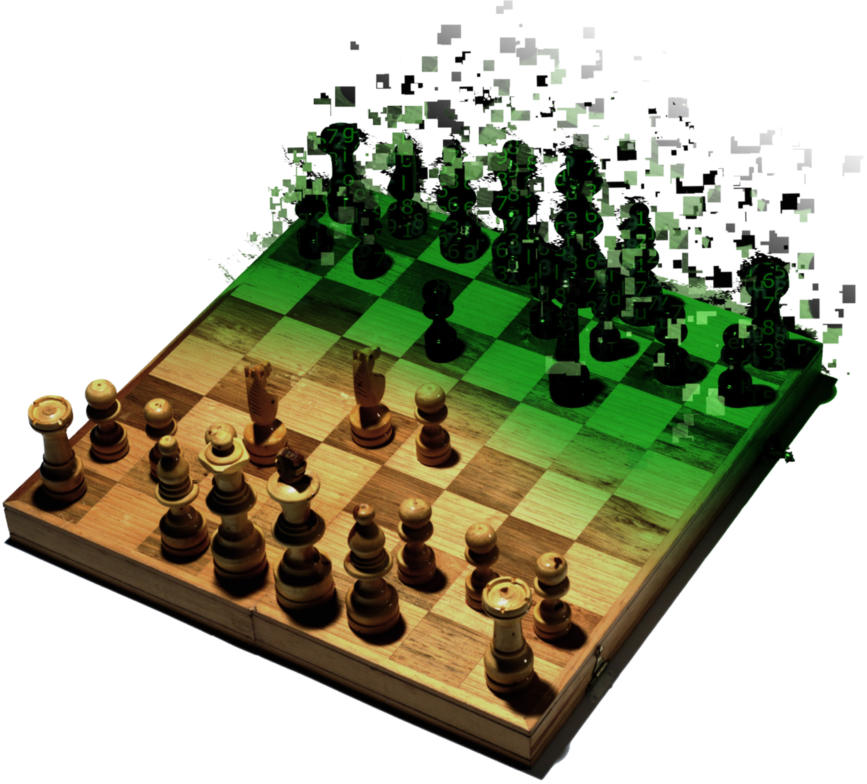
Puolustusvoimien tutkimuslaitos
Julkaisuja 10

GAME CHANGER
Structural transformation of cyberspace

Juha Kukkola | Mari Ristolainen | Juha-Pekka Nikkarila



Finnish Defence Research Agency Publications 10
Puolustusvoimien tutkimuslaitoksen julkaisuja 10

GAME CHANGER
Structural transformation of cyberspace

Juha Kukkola
Mari Ristolainen
Juha-Pekka Nikkarila

FINNISH DEFENCE RESEARCH AGENCY
PUOLUSTUSVOIMIEN TUTKIMUSLAITOS

RIIHIMÄKI 2017

Cover design: Photographer/Graphic Designer
Niko Savola

ISBN 978-951-25-2953-7 (print)
ISBN 978-951-25-2954-4 (PDF)
ISSN 2342-3129 (print)
ISSN 2342-3137 (online publication)

Finnish Defence Research Agency
Puolustusvoimien tutkimuslaitos

Juvenes Print
Tampere 2017

Contents

Tiivistelmä

Game Changer – artikkelikokoelman tekstit käsittelevät suunnanmuutosta kansainvälisen kybertilan (*cyberspace*)[1] rakenteellisessa hallinnassa. Tarkastelemme tutkimuksissamme tämän muutoksen vaikutuksia tulevaisuuden kybertilaan ja väitämme vaikutusten olevan mahdollisesti hyvin merkittäviä. Lähestymme tätä suunnanmuutosta poikkitieteellisesti Venäjän kulttuurin- ja yhteiskunnantutkimuksesta tietojenkäsittely- ja informaatiotieteiden sekä matematiikan kautta sotatieteisiin. Artikkelikokoelman tekstit on järjestetty kirjoitusjärjestykseen alkaen syksystä 2016 ja loppuen syksyyn 2017. Ajallisen järjestyksen tarkoituksena on kuvata sitä haasteellista tutkimusprosessia, jossa tutkija toimii tutkiessaan ajankohtaista ja jopa päivittäin muuttuvaa tutkimuskohdetta. Uuden tiedon suhteuttaminen jo olemassa olevaan ja niiden yhteisvaikutusten arvioiminen tekee tutkimusprosessista ison palapelin kasaamista, jonka lopullinen tavoitekuva on tuntematon. Viimeisen artikkelin kirjoitusprosessissa on ollut käytettävissä huomattavasti enemmän tietoa kuin ensimmäisen, mutta jokaista artikkelia tarvitaan ymmärtääkseen seuraavan. Tässä suomenkielisessä yhteenvedossa kuvataan artikkelikokoelman kirjoitusten sisällöt tiivistetysti. Olemme pyrkineet suomentamaan käytetyt kyberkäsitteet ja antamaan valitsemiemme käsitteiden käytölle tarkennuksia ja selityksiä alaviitteissä.

Pitäisikö ”RuNet 2020” ottaa vakavasti?

Kesällä 2016 Venäjän viestintäministeriö ilmoitti tavoitteekseen luoda vuoteen 2020 mennessä kansallinen riippumaton internet – RuNet (sanoista *Russian Internet*). Venäjän viestintäministeriön mukaan internetin venäläinen osa irrotetaan globaalista verkosta venäläisen ”kriittisen infrastruktuurin suojaamiseksi”. Tämä pyrkimys on hyvin

[1] Englanninkielinen *cyberspace* kääntyy suomeksi hyvin monella eri tavalla: kyberavaruus, kybermaailma, kybertoimintaympäristö, kyberympäristö, kybertila jne. Suomenkielisten käsitteet ovat epätarkkoja, monimerkityksellisiä ja vakiintumattomia. Parhaillaan kyberkäsitetutkimusta ja -määrittelyä tehdään sekä Puolustusvoimien sisällä että viranomais- ja asiantuntijatasolla. Tässä suomenkielisessä tiivistelmässä käytämme käsitettä ”kybertila”, koska mielestämme se avaa suomenkieliselle lukijalle paremmin tutkimamme ilmiön olemusta. Maailma, avaruus ja ympäristö ovat liian abstrakteja kun kyseessä on määrätty tila, jossa sen osilla ja tapahtumilla on suhteellinen paikka toisiinsa nähden ja jonka rakennetta on mahdollista fyysisesti muokata ja rajata.

erilainen kuin maailmanlaajuinen tavoite luoda ”avoin ja turvallinen” sekä luottamukseen perustuva internet. Artikkelikokoelman ensimmäisessä artikkelissa kysytäänkin pitäisikö ”RuNet 2020” ottaa vakavasti ja jääkö meiltä jotain huomaamatta, koska ymmärryksemme kyber/informaatioturvallisuudesta[2] poikkeaa venäläisestä. Niin sanotussa ”läntisessä” ajattelussa keskitytään turvaamaan tiedon ja datan vapaa liikkuvuus, joka perustuu avoimeen globaaliin verkkoon. Tässä kybertilassa westfalenilainen suvereniteetti on lähes mahdoton ajatus. Avoin internet perustuu laajalla kansainvälisellä yhteistyöllä saavutettavaan avoimeen kybertilaan, jossa toimijoiden turvallisuudesta huolehtii jokainen itse suojaamalla omat järjestelmänsä. Kuitenkin Venäjällä asia nähdään lähes päinvastoin – ”digitaalinen suvereniteetti” on mahdollista saavuttaa ja suljettu riippumaton verkko on tavoitetila, joka takaa kansallisen turvallisuuden. Venäläisen ajattelutavan mukaan kyber/informaatiotilaa hallitsevat ”muut maat”, jotka tähtäävät Venäjän kansallisen turvallisuuden horjuttamiseen.

Artikkelissa esitetään, että venäläisen ajattelutavan ja toiminnan analysointi läntisten käsitteiden kautta estää meitä ymmärtämästä, kuinka voimakas Venäjän pyrkimys on ”digitaaliseen suvereniteettiin” ja näkemästä, kuinka paljon Venäjä haluaa haastaa USA-vetoisen maailmanjärjestyksen. Aikaisempaa tutkimusta venäläisestä suljetusta kansallisesta verkosta ei juuri ole, koska sitä on läntisessä ajattelussa pidetty järjettömänä toteuttaa – pelkkänä propagandana. Toisaalta RuNet – suljettuna suvereenina kyber/informaatiotilana – on uusi ja kokoajan kehittyvä konsepti, joka koostuu hyvin monenlaisista osista, joiden monimutkaisuutta ja yhteisvaikutuksia pitää tutkia eri näkökulmista.

Ensimmäisessä artikkelissa kuvataan lyhyesti RuNet-ajattelun taustaa. RuNet-termiä on käytetty lähes kaikesta mikä tapahtuu internetissä

[2] Koska kirjoituksessa käsitteellään venäläistä ajattelua, käytämme suomeksi yhdistelmää ”kyber/informaatio”. Monien tutkijoiden mukaan Venäjä-yhteydessä ei pitäisi puhua ”kyberistä” lainkaan. Virallisissa venäjänkielisissä asiakirjoissa ei juurikaan mainita sanaa ”kyber”, vaan se korvataan etuliitteellä ”informaatio-”. Kyberturvallisuus ei ole synonyymi informaatioturvallisuudelle, mutta venäläinen informaatioturvallisuuden käsite pitää sisällään myös kyberturvallisuuden. Läntisen ajattelutavan mukaan ”kyberpuolustus” on ensisijaisesti teknistä puolustautumisesta teknisiä uhkia vastaan. Venäläisen ajattelutavan mukaan informaatio on sekä ase, jolla vaikutetaan että kohde, jota puolustetaan. Venäjä toimii ”informaatiotilassa” (*informatsionnoe prostranstvo*) ja/tai ”informaatioympäristössä” (*informatsionnaja sfera*), jossa sillä on sekä teknistä että tiedollista hyökkäys- ja puolustuskapasiteettia.

venäjänkielellä ja joka linkittyy jotenkin venäläiseen kulttuuriin riippumatta fyysisestä sijainnista. RuNet on alkuperäiseltä merkitykseltään suhteellisen suljettu ja vapaasti kehittynyt venäjänkieleen perustuva kyber/informaatiotila, joka on kehittynyt kyrillisillä kirjaimilla palveluja tuottavana vaihtoehtona hallitsevan englanninkielisen internetin rinnalle. RuNetin tavoite on ylläpitää venäläisiä kulttuurisia ja hengellisiä arvoja ja korostaa ”venäläistä tapaa” tehdä asioita. Jo RuNetin alkuperäisessä ideassa tiivistyy tietynlainen itsenäisyys ja riippumattomuus ”läntisestä” maailmasta. Viime vuosien aikana tämän vaihtoehtoisen informaatiotilan kontrollia on alettu kiristää. RuNetista on alkanut kehittyä vallankäytön väline, eräänlainen informaatiovaikutusalue, jonka kautta saa ”oikeaa ja turvallista tietoa” venäjäksi. Toisin sanoen RuNet ilmiönä on alkanut muuttua vaihtoehtoisesta sosiaalisesta tilasta valtiojohtoiseen ”suljettuun ja turvalliseen” kyber/informaatiotilaan, joka edistää ja mahdollistaa ”digitaalisen suvereniteetin”.

Artikkelissa kartoitetaan millaisiin toimenpiteisiin Venäjällä on ryhdytty ”digitaalisen suvereniteetin” saavuttamiseksi kielen, kulttuurin ja ”moraalisen puhtauden” saralla, lainsäädännössä, kansallisten ohjelmistojen kehitys- ja käyttöönotossa, uusien liittolaisten hankinnassa sekä listataan mahdollisia teknisiä suunnitelmia. Lopuksi artikkelissa pohdiskellaan miltä globaali kyber/informaatiotila voisi näyttää, jos Venäjä onnistuu tavoitteessaan luoda vuoteen 2020 mennessä kansallinen riippumaton RuNet eli pakottaa omien verkkojen reititys Venäjän alueelle ja säilyttää toimintakyky globaalin internetin ulkopuolella. Tämä artikkeli on toiminut tienviitoittajana kokoelman muille artikkeleille, joissa ”RuNet 2020” on otettu vakavasti ja nähty tutkimisen arvoisena ilmiönä.

RuNet 2020 – taistelun peruselementtien soveltaminen kybertilassa?

Artikkelikokoelman toisen artikkelin lähtökohtana on ensimmäisessä artikkelissa todettu tulos, että Venäjä on aloittanut kansallisen verkon sulkemisprosessin. Käytännössä näin toimimalla Venäjä saavuttaisi kyvyn kytkeä tarvittaessa Venäjän kansallinen verkko irti maailmanlaajuisesta internetistä. Samalla suljetun kansallisen verkon operatiivinen kyky ei kokisi merkittävää häiriötä. Artikkelissa selvitetään, mitkä voisivat olla kansallisen verkon sulkemisprosessin sotilaalliset tavoitteet. Tutkimusväitteenä on, että RuNetin perustana olevaa strategiaa voidaan analysoida käyttäen perinteistä sodankäynnin taktiikkaa ja erityisesti käyttäen taistelun peruselementtejä: tulta, suojaa ja liikettä. Artikkelissa analysoidaan kuinka RuNet voisi vaikuttaa Venäjän kannalta taistelun peruselementteihin kyber/informaatiotilassa. Tutkimuksessa päätellään, että teknisesti onnistuessaan kansallinen suljettu verkko tulee parantamaan suhteellista liikehdintäkykyä, suojaa ja tulivoimaa suhteessa avoimiin verkkoihin. Tutkimustuloksena esitetään, että Venäjän sotilaallinen tavoite onkin parantaa erityisesti omaa liikehtimiskykyä suhteessa muihin toimijoihin.

Tutkimustuloksen analysointia syvennetään peliteoreettisen tarkastelun avulla koskemaan muita Venäjän mahdollisia strategisen tason tavoitteita, joita ovat kirjoittajien alkuperäislähteiden analyysin perusteella maailmanlaajuisen sotilaallisen tasapainon haastaminen ja läntisen maailmanjärjestyksen horjuttaminen. Peliteoreettisessa tarkastelussa yhtenä tärkeänä tekijänä on, pystyykö Venäjä saamaan liittolaisia tai seuraajia verkkojen sulkemiselle. Mikäli liittolaisia ei tulisi ollenkaan tai jos tulisi yksi merkitykseltään pieneksi luokiteltu seuraaja, merkittävimpänä toimintalinjana (tai tavoitteena) olisi sotilaallisen tasapainon haastaminen. Tällöin Venäjän kannalta suurimmiksi hyödyiksi jäisivät oman ja mahdollisen liittolaisen suhteellisen liikkuvuuden parantaminen kyber/informaatiotilassa suhteessa muihin toimijoihin. Mikäli Venäjä onnistuisi saamaan useita tai merkittäviä liittolaisia, olisi tilanne toinen. Tämä pakottaisi muut toimijat reagoimaan ja reagoinnin suunnan perusteella pystytään hahmottelemaan kolme skenaariota, joiden kautta tavoitteena olisi läntisen maailmanjärjestyksen horjuttaminen. Nämä skenaariot nimetään artikkelissa ominaisuuksiensa ja seurauksiensa perusteella seuraavasti: ”kestävä avoimuus” (*resistant openness*), ”merkittävästi sulkeutunut” (*substantially closed)* ja ”hermostunut avoimuus” (*nervous openness*). Esitettyjen skenaarioiden kautta artikkeli nostaa esiin uusia tutkimuskohteita maailmanlaajuisen tilannetietoisuuden parantamiseksi.

Mitkä ovat avoimen verkon yhteisön valinnat ja niiden seuraukset vastakkainasettelussa suljetun verkon valtion kanssa?

Kolmas artikkeli jatkaa kansallisten suljettujen verkkojen sotilaallisten vaikutusten tutkimista avoimen verkon yhteisön näkökulmasta pohtimalla, mitkä ovat avoimen verkon yhteisön toimintamahdollisuudet tässä uudessa tilanteessa.

Venäjän virallisten strategioiden, doktriinien ja poliittisten ohjelmien analyysin kautta artikkelissa määritellään aluksi neljä erilaista toimintalinjaa, joiden kautta Venäjä mahdollisesti pyrkii hallitsemaan kybertilan sotilaallista operaatioulottuvuutta eli kyberulottuvuutta[3]. Näitä toimintalinjoja ovat: digitaalisen suvereniteetin lisääminen, kyber/informaatiotilan käsitteellinen hallinta, kybertilan tekninen valmistelu ja avointen verkkojen heikkouksien hyödyntäminen. Artikkelissa väitetään, että näiden toimintalinjojen kautta suljetun verkon valtio pystyy pakottamaan avoimen verkon yhteisön reagoivaan tilaan ja näin saavuttamaan sotilaallisen etulyöntiaseman asymmetristen rintamalinjojen muodossa. Suljetun ja avoimen verkon rajapintaan syntyy rintamalinja, joka vaikuttaa erityisesti liikenteeseen suljettuun verkkoon päin. Lisäksi suljetun verkon sisälle syntyy puolustuksellisia rintamalinjoja. Koska vastaavia rintamalinjoja ei ole avoimen verkon sisällä, tuloksena ovat asymmetriset rintamalinjat (*asymmetric frontlines*). Artikkelissa analysoidaan neljän erilaisen hyökkäysvektorin kautta hyökkäyksellisten ja puolustuksellisten operaatioiden toimintamahdollisuuksia avoimissa ja suljetuissa verkoissa.

Skenaarioanalyysin kautta artikkelissa arvioidaan avoimen verkon yhteisön strategisia valintoja ja niiden seurauksia, kun kyseessä on mahdollinen vastakkainasettelu suljetun verkon valtion kanssa. Artikkelissa määritellään kaksi tekijää, jotka vaikuttavat avoimen verkkoyhteiskunnan päätöksentekoon: 1) ymmärretäänkö suljetun verkon valtion tavoitteet ja niiden muodostama uhka; 2) kuinka tiukasti avoimen verkon yhteisö on valmis pitämään kiinni arvovalinnoistaan ja puolustamaan avoimuutta. Näiden tekijöiden kautta saadaan eroteltua neljä erilaista avoimen verkon yhteisön päätöksentekoa kuvaavaa prosessia – valintoja ja niiden seurauksia: 1) ”hermostunut avoimuus” (*nervous openness*); 2) ”idealistinen avoimuus” (*idealistic openness*); 3) ”merkittävästi sulkeutunut” (*substantially closed);* 4) ”kestävä avoimuus” (*resistant openness*). Avoimen verkon yhteisön valintojen ja niiden

[3] Käytämme artikkeleissa käsitettä ”kyberulottuvuus” (*cyber domain*), vaikka se on sekä suomeksi että englanniksi kiistelty, ristiriitainen ja täysin vakiintumaton käsite. Määritelmämme mukaan kyberulottuvuus on kybertilan sotilaallinen toimintatila (sotilaallinen toimintaympäristö tai taistelutila), joka lävistää kaikki muut konventionaaliset ulottuvuudet (maa, meri, ilma ja avaruus). Näkemyksemme mukaan kyberulottuvuudesta voidaan erottaa vielä erityyppisiä osia eli ”kybertaistelukenttiä” (*cyber battlefield*), joilla käydään taisteluja taktisten ja operatiivisten päämäärien saavuttamiseksi. Kokoelman viimeisimmissä artikkeleissa käsitellään vielä kybertaistelukentän osatekijöiden – tilan ja ajan – muokkausta.

seurausten analyysi vaihtavat edellisen artikkelin tarkastelukulman ja syventävät sen tuloksia.

Artikkelissa tarkastellaan lähemmin ns. ”kestävän avoimuuden” mahdollisia toimintamalleja ja esitetään miten niiden tulisi vastata aikaisemmin esitettyihin suljetun verkon valtion toimintalinjoihin. Esitetyt toimintamallit ovat avoimuuden edistäminen, konseptuaaliset muutokset, teknologian kehittäminen ja resurssien uudelleenorganisointi. Näiden lisäksi artikkelissa kuvataan miten erilaiset avoimen verkon yhteisön päätöksentekoa kuvaavat tilat vaikuttavat mahdollisessa eskalaatiotilanteessa ja millaisia riskejä niistä aiheutuu.

Tulevaisuuden kybertaistelukenttien asymmetriset rintamalinjat

Neljäs artikkeli jatkaa aikaisemmin havaittua avoimien ja suljettujen verkkojen eroista nousevan sotilaallisen epäsuhdan tarkastelua. Sen tavoitteena on pohtia, miltä tulevaisuuden kybertaistelukenttä voisi näyttää, mikäli Venäjä loisi valmiudet sulkea kansalliset verkkonsa tavoitellessaan ”digitaalista suvereniteettia”. Tutkimus tarjoaa venäläisiä alkuperäislähteitä käyttäen päivityksen tilannekuvaan Venäjän viimeaikaisista hallinnollisista ja lainsäädännöllisistä hankkeista, jotka tähtäävät kansallisen, alueellisesti rajatun informaatiotilan hallintaan. Näiden, ja merkittävien venäläisten akateemikkojen kirjoitusten pohjalta, esitetään Venäjän mahdollisesti valmistautuvan verkkojensa sulkemiseen käyttäen Border Gateway Protocol (BGP) -protokollaa ja Software Defined Networking (SDN) teknologiaa yhdistettynä kotimaiseen teknologiaan sekä hallinnollisiin määräyksiin ja lainsäädäntöön. Tutkimuksen lähtökohtana on, että tällä hankkeella on sotilaallinen luonne.

Artikkeli tarkastelee suljettujen verkkojen suhdetta avoimiin verkkoihin sotilasstrategisella tasolla ”kyberasymmetrian” käsitteen kautta. Se perustuu kybertaistelukenttien (*cyber battlefield*)[4] tila ja aika osatekijöiden muokkaamiseen kontrolloimalla digitaalisesti ja fyysisesti internetin kansallisia ja territoriaalisia osia. Näillä toimenpiteillä on vaikutusta toiminnanvapauteen, päätöksentekoon ja tilannekuvaan, joiden

[4] Vrt. edellinen alaviite.

epäsuhta avoimen ja suljetun verkon toimijan välillä johtaa asymmetriaan. ”Kyberasymmetria” tarjoaa perinteisestä ei-valtiollisiin toimijoihin ja määrättyihin keinoihin perustuvasta näkemyksestä poikkeavan hyödyllisen, venäläiseen ajatteluun sopivan, tarkastelukulman.

Asymmetrian tutkimiseen käytetään skenaarioanalyysia ja ennustavaa mallintamista. Niiden avulla paikannetaan kolme erityyppistä kybertilaa, jotka syntyvät sulkemisprosessin seurauksena: suljettu (*closed subspace*), avoin (*open subspace*) ja pirstaloitunut (*fractured subspace*). Näiden kohdatessa syntyy kybertaistelukenttiä, joita tarkastelemalla tutkimuksessa todetaan kybertaistelukentän tila ja aika osatekijöiden muokkaamisen johtavaan huomattavaan etuun suljettujen verkkojen toimijoiden osalta. Tätä havaintoa syvennetään tarkastelemalla avoimien ja suljettujen verkkojen välisiä rintamalinjoja hyökkäyksellisten ja puolustuksellisten operaatioiden kautta. Tutkimus toteaa, että rintamalinjoilla on selvä asymmetrinen luonne niiden rajoittaessa merkittävästi avoimen verkon toimijoiden hyökkäysoperaatioita samalla, kun suljetun verkon toimija kykenee operoimaan suhteellisen vapaasti avoimien verkkojen syvyydessä. Tällä on suora vaikutus kyberpelotteen ja eskalaationhallinnan strategioihin niin sodan kuin rauhan aikana tai niiden välissä.

Artikkelin analyysin perusteella voidaan väittää, että kybertila sodankäynnin ulottuvuutena ja taistelukenttänä on muokattavissa ja sen kautta on mahdollisuus saavuttaa merkittävä sotilaallinen etu jo ennen avoimen konfliktin syttymistä. Kansallisten verkkojen sulkeminen johtaa ”kyberasymmetriaan” ja se tulisi ottaa huomioon tutkittaessa kybertilan sotilaallista käyttöä nyt ja tulevaisuudessa.

Suljettujen ja avointen verkkojen välillä käytävien kyberoperaatioiden epätasapainon matemaattinen mallintaminen

Viidennessä artikkelissa (laajennettu abstrakti) esitetään matemaattinen malli kuvaamaan suorituskyvyn muutosta, joka johtuu suljettujen ja avointen kansallisten verkkojen välille muodostuvista asymmetrisista rintamalinjoista. Suorituskyky esitetään todennäköisyytenä torjua vihamielinen operaatio omassa verkossa. Mallintamisen lähtökohtana on aikaisemmissa tutkimuksissa erittäin todennäköisenä pidetty suljetun tai jopa useiden suljettujen kansallisten verkkojen muodostuminen lähitulevaisuudessa. Mallissa käytetyn menetelmän avulla verkkojen sulkeutumisen vaikutuksia voidaan analysoida tarkemmin. Mallin avulla pystytään havainnollistamaan kansallisten verkkojen välille syntyvää epätasapainoa kyvyssä käydä kyberoperaatioita. Tutkimus on, kirjoittajien käsityksen mukaan, ensimmäinen verkkojen sulkeutumisen vaikutuksia matematiikan menetelmin selvittävä julkaisu. Artikkelin tulokset parantavat tilannetietoisuutta verkkojen sulkeutumisprosessin vaikutusten hahmottamisessa. Kirjoittajat pitävät sulkeutumisprosessin tutkimista tärkeänä ja pyrkivät omalla tutkimuksellaan myös näyttämään suuntaa tulevalle tutkimukselle.

Kyberasymmetria – kohti uudenlaista strategista ajattelua?

Artikkelikokoelman viimeisessä artikkelissa tavoitteena on kehittää edelleen ”kyberasymmetrian” käsitettä rakentamalla sille vahva teoreettinen pohja ja haastamalla perinteiset sotilaalliset asymmetriakäsitykset aikaisempia artikkeleita syvällisemmin. Perustuen neoklassisesta realismista ja strategisen kulttuurin käsitteestä muodostettuun teoreettiseen viitekehykseen artikkeli esittää ”rakenteellisen kyberasymmetrian” käsitettä kuvaamaan kansallisten, territoriaalisten verkkojen sulkemisesta syntyvää sotilaallista etua. Läntiseen tutkimukseen perustuvan kybertilan ja eri voimateorioiden analyysin kautta esitetään kybervoiman (*cyber power*) määritelmäksi: “Toimijan kyky vaikuttaa toisiin toimijoihin kybertilassa tai sen kautta ja muokata kybertilaa omaksi edukseen preferenssiensä mukaan.” Kybervoiman sotilaallista luonnetta tarkastellaan vertaamalla sitä aikaisempiin kirjoituksiin voimankäytöstä ja todetaan sen poikkeavan osiltaan tavanomaisen sotilaallisen voimankäyttöön liittyvistä näkemyksistä. Samalla todetaan, että kybervoiman käyttö, kuten muukin sotilaallisen voiman käyttö, on kulttuurisidonnaista eli riippuvaista käyttäjän ymmärryksestä voiman luonteesta, ympäristöstä ja tavoitteista. Tässä prosessissa merkittävä tekijä on strategialla, joka on osa voimamääritelmän ”kykyä vaikuttaa.”

Asymmetrian tarkastelu aloitetaan kirjallisuuskatsauksella läntiseen ajatteluun, jonka perusteella todetaan käsityksen olevan rajoittunut määrättyihin keinoihin, toimijoihin ja näkökulmaan. Havaintojen pohjalta ja kybertilan muokkaamisen vaikutusten ymmärtämiseksi ”rakenteellinen kyberasymmetria” (*structural cyber asymmetry*) esitetään kybertilan ominaisuudeksi, joka syntyy muokkaamalla sen sääntöjä ja rakennetta. Muokkaamalla tilaa voidaan luoda etu, joka ei ole lähtökohtaisesti puolustuksellinen tai hyökkäyksellinen, mutta edellyttää valtiotason resursseja. Muokkaustoimet voivat tapahtua fyysisellä, syntaktisella tai semanttisella tasolla teknologian, normien ja politiikan kautta. Ne vaikuttavat tilannetietoisuuteen, toiminnanvapauteen, päätöksentekoon ja kohteiden suojaan. Asymmetria syntyy näiden tekijöiden epäsuhdan tuloksena. Artikkeli väittää, että sulkemalla kansalliset verkkonsa konfliktin osapuoli saavuttaa selvän pelote-edun, kykenee kontrolloimaan konfliktin etenemistä ja voi uhata vastustajaansa voima-asemasta käsin.

Artikkeli perustuu länsimaiseen kirjallisuuteen, mutta lähtökohtana on todellisen kybertilan ilmiön kuvaaminen. Se, miten käsite auttaa ymmärtämään esimerkiksi venäläistä strategista ajattelua ja toimintaa, tulee todentaa empirian kautta. Samoin on jatkettava mallintavaa tutkimusta verkkojen sulkemisen osalta. ”Rakenteellinen kyberasymmetria” ei ole kulttuurinen tai toimijaan sidottu käsite vaan apuväline verkkojen sulkemisen vaikutusten ymmärtämiseksi.

Suunnanmuutos

Game changer – kokoelman artikkeleissa esitetään vahva todistusaineisto siitä, että Venäjä (ja mahdolliset muutamat muut valtiot) pyrkivät internetin kansallisten osien valtiolliseen hallintaan ja tarvittaessa sulkemiseen. Tämä voi johtaa kirjoittajien mukaan kyberulottuvuudessa sotilaalliseen asymmetriaan verkkonsa sulkevien valtioiden eduksi. Muodostuva asymmetria poikkeaa aikaisemmasta läntisestä ymmärryksestä. Kyberasymmetriaa luodaan usean eri toimintalinjan kautta ja se on kytköksissä internetin luonteesta käytävään kamppailuun ja laajemmin kansainvälisen voimatasapainon muutokseen. Kyseiseen asymmetriaan vastaaminen vaatii laaja-alaista, monitieteellistä tutkimusta teknisestä strategiselle ja poliittiselle tasolle ilmiön vaikutusten ja sen taustalla olevien toimien ymmärtämiseksi. Tutkimus on välttämätöntä, jotta asymmetriaan kyetään vastaamaan riittävän ajoissa harkituilla keinoilla ja menetelmillä. Tämä on ainoa tapa välttää asymmetriasta johtuva turvattomuuden lisääntyminen. Ainoastaan kansainvälisellä yhteistyöllä kykenemme säilyttämään internetin luonteen avoimena, turvallisena ja vakaana.

Introduction

Juha Kukkola
Mari Ristolainen
Juha-Pekka Nikkarila

game changer
- a newly introduced element or factor that changes an existing situation or activity in a significant way (Merriam-Webster 2017)

This collection of papers was never intended to be a single publication and does not reflect the results of a well-planned, generously-funded, or lengthy research project. The collection represents a freely developing scientific research process at its best. It shows what happens when researchers from radically different fields of study are given the opportunity to take an interest in each other's work and start to think outside their own boxes – most likely it is the first ever military science paper collection written by a humanist, a physicist and a social-scientist!

During the autumn of 2016 a newly hired 'cyber researcher' at the Finnish Defence Research Agency – a Russian poetry and border researcher in her former life – started to plan her own 'cyber phenomena' research topics and remembered that during the summer she had heard something about a 'Russian national network' which was planned to be disconnected from the global network by 2020. Her new colleagues found it rather amusing when she asked questions and tried to find out if somebody knew something about it. Nobody did. It was simply considered too silly or pure propaganda. Nevertheless, stubbornly she found the topic too interesting to pass up. The first paper of this collection started out as a working paper intended for her superior to read and to reflect whether this could be something worth studying in the future. Around the time the first draft was finished, the Russian Information Security Doctrine was signed by Vladimir Putin on December 5, 2016. The notion where Russia openly aimed "to deploy a national system of managing the Russian segment of the Internet" fitted her paper perfectly where she had already listed several measures that had been done in

Russia in order to develop a ‘national network’. She was encouraged to send her abstract to several conferences. After refusals, finally, her abstract entitled: “Should ‘RuNet 2020’ be taken seriously? Contradictory views about cybersecurity between Russia and the West” was selected for submission as an academic paper at the 16th European Conference on Cyber Warfare and Security 2017 (ECCWS 2017). In this paper she asks if we are missing something fundamental about cybersecurity because we see cyberspace and cybersecurity from our Western ‘open and shared’ perspective. She argues that in order to understand new cybersecurity threats we must acknowledge the essential differences between Russia and the West and look beyond them. In this paper she introduces the Russian approach to digital sovereignty and cybersecurity and presents a futuristic view of the global cyberspace of 2020 with or without RuNet. In this collection the original ECCWS 2017 version of the paper is published, whereas an updated version is forthcoming in the Journal of Information Warfare in the autumn of 2017.

The paper was also read by her colleague, an open-minded, engineer-officer, and a physicist, who just a couple of days before the Christmas holidays came-up with an idea on how to develop the topic further – and the second paper – “RuNet 2020 – Deploying traditional elements of combat power in cyberspace?” was swiftly launched between Christmas and New Year. Their superior considered both the authors and the paper provocative but allowed them to submit it to the International Conference on Military Communications and Information Systems (ICMCIS 2017) where it was also accepted. This paper was their first attempt to analyse the military motivation and outcomes of the network closure process. In this paper they analysed the possible military aims of ‘closed network nations’ and came to the conclusion that the goal is related to enhancing military capabilities (e.g. the basic elements of combat power) when compared to open networks. In other words, they argued that it is likely that the motivation behind a closed network nation is to achieve a higher operational capability than ‘open network’.

Also just before Christmas she was contacted by an enthusiastic PhD-candidate from the National Defence University, an officer-strategist and social-scientist, who was starting his dissertation study on Russian cyber power. The two asked him to read and comment on their ‘combat power’ paper. His comments were extremely critical and pointed out what was desperately missing in the paper. As a result, the three decided to elaborate the topic more and to write a third paper together. Their flexible superior encouraged them to aim high and submit the paper "Confrontation with a Closed Network Nation: Open Network Society's Choices and Consequences" to the Military Communications (MILCOM 2017) conference, where it was – to all of their surprise – accepted. In this paper they continue to analyse the outcomes of the closing process from an open network society's point of view and show how a nation with a closed network can shape the cyber domain to gain an advantage and thus may control the cyber domain and be able to force an open network society into a reactive mode. They determine open network society's choices and their consequences in the case of escalation and potential confrontation. Moreover, their aim was to deepen the understanding of how closed national networks can impact the future cyber domain from the military perspective. They argue that Russia is currently manipulating the cyber domain through four identified lines of effort that may result in advantages in the form of asymmetric frontlines on cyber battlefields.

As in any innovative research process more questions than answers are raised. Moreover, the Strategy on the Development of Information Society in the Russian Federation for 2017–2030 was signed in May 9, 2017. Yet again, this document reinforced their findings and gave a strong impetus to learn more. The third paper led to the next and they found themselves deeper and deeper in the topic of asymmetry on cyber battlefields. The forth paper "Asymmetric frontlines of cyber battlefields" was accepted by the International Command and Control Research and Technology Symposium (ICCRTS 2017)[1]. The aim of the fourth paper was to consider how a future cyber battlefield could look. They show how 'digital sovereignty' could be technically structured, what kinds of policies it would require and how it would affect future cyber battlefields. 'Digital sovereignty' combined with the ambiguity of conflict creates an asymmetry that can be exploited and used for shaping the cyber domain

[1] Editor's note: This paper won the best paper award at the ICCRTS 2017.

into a future battlefield with ‘asymmetric frontlines’. They claim that the conventional understanding of asymmetry in cyberspace which is based on the problem of attribution will become outdated. Their analysis demonstrates how time and space variables form a base for asymmetry in the future cyber battlefield. By studying on the one hand the creation of asymmetry and on the other its effects on the freedom of action, decision making and situation awareness of belligerents, they analyse the creation and dynamics of ‘cyber asymmetry’.

Meanwhile, the first papers were presented in public. Initially, the audience was confused, but they were deeply interested in their work and the authors received encouraging feedback from ‘top level’ military scholars. As the theme was also discussed during coffee breaks, a progressive mathematician in the Finnish Defence Research Agency also decided to take on the challenge. He showed how this phenomenon could be calculated and the fifth paper (extended abstract) “Modelling the imbalance of cyber operations between closed and open national networks” was rapidly written and submitted to the annual conference of the International Society for Military Sciences (ISMS 2017). This paper introduces a mathematical model to describe asymmetric frontlines. When considering defence, the model gives the capability as a probability for denying adversarial operations in a friendly network.

At this point the originally ‘irrational’ idea started to seriously develop into a theory and the officer-strategist decided to focus his PhD-dissertation on the theme and ask whether Russian cyber power consists of shaping and delineating cyberspace with technical, administrative and political tools. During his summer holidays he wrote the sixth paper “Cyber Asymmetry – Towards New Strategic Thinking?” which concludes this collection. In this working paper and a draft chapter of his future dissertation he argued that the effort of some states to build sovereignty in cyberspace (digital sovereignty), is in fact an intentional project to create a strategic asymmetric advantage. This advantage is both defensive and offensive and gives these states a definite advantage on a strategic level vis-à-vis nations who decide to rely on a free and open Internet. This paper represents a conceptual opening on the theme and develops a method for further analysis of cyber asymmetry created by intentionally closing national cyberspace. These thoughts were reinforced when a state programme titled ‘The Digital Economy of the Russian Federation’, was signed in July 28, 2017. This programme presents a ‘road-map’ setting the task for Russia to become digitally sovereign by 2020 and for Russia to be one of the world’s leading countries in the field of information security by 2024. One can only speculate as to how the realization of this task is planned.

To study an ongoing phenomenon is inspiring but also challenging. Everything that is written today may be outdated tomorrow. This collection of papers symbolises a process where almost every day a new piece of the puzzle needs to be fitted in. Sometimes the whole picture seems to change; sometimes it becomes clearer. Because of this enduring process, the papers contain some repetition and are not linguistically perfect. Yet, at some point somebody got the idea to print all of these as a collection – just to grab the academic and military communities’ attention.

The group of three is very grateful for the chance to work together supported by both the Finnish Defence Research Agency and the National Defence University. Office hours were not enough to write these papers. Still for the past year, they have been able to work passionately in order to enhance the public understanding of some of the strategic processes threatening the Internet as we know it today. They consider the potential structural changes of cyberspace as a ‘game changer’ that needs to be comprehended and studied further. This collection of papers serves as an open invitation to join the group and to suggest new aspects to the research. The story does not have an ending yet.

Should ‘RuNet 2020’ be taken seriously? Contradictory views about cybersecurity between Russia and the West

Mari Ristolainen

Abstract

The Internet has been governed by freedom and happiness with a strong emphasis on connection, sharing, and openness – reflecting the worldviews of the computer scientists who first built it. Few people seriously consider the possibility that RuNet – the Russian segment of the Internet – could firstly, be disconnected from the global Internet by 2020; and secondly, see it as a threat to cybersecurity or even an instrument of deterrence. However, the original worldview may not be the new norm of the evolved cyberspace. Cyberspace is increasingly becoming more fragmented and linguistically divided. In its recently approved Information Security Doctrine, Russia openly aims “to deploy a national system of managing the Russian segment of the Internet”. In the Russian way of thinking, full digital sovereignty is possible and necessary for national security purposes. ‘RuNet 2020’ would be closed, safe and fully controlled by the state. The Russian aim is to create an independent state information system – ‘a back-up copy’ – that ensures the network’s overall stability by controlling the Internet routing architecture inside Russia. A more tightly regulated and secure ‘information space’ will ensure stronger defence against external attacks. This paper asks if we are missing something fundamental about cybersecurity because we observe cyberspace and cybersecurity from our Western ‘open and shared’ perspective. The argument states that in order to understand the new threats of cybersecurity we must acknowledge the essential differences between Russia and the West and look beyond them. This paper introduces the Russian approach to digital sovereignty and cybersecurity and presents a futuristic view of the global cyberspace of 2020 with or without RuNet.

Keywords: Digital sovereignty, governance of cyberspace and/or information space, cybersecurity, Russia, RuNet

The first version of this paper was published and presented at the 16th European Conference on Cyber Warfare and Security 2017 (ECCWS 2017), Dublin, Ireland, June 29–30, 2017.

1 Introduction

In an idealistic Western[1] mind-set, the Internet is governed by freedom and happiness with a strong emphasis on connection, sharing, and openness – reflecting the worldviews of the computer scientists who first built it. The Internet was designed to share information and in this view it is threatened by censorship and control. Moreover, the entire cyberspace is envisioned as a space where borders and states are no longer able to adapt to the so-called Westphalian state system [1], [2]. Digital sovereignty is neither possible nor desired in the cybersecurity model of ‘open, safe and secure’ cyberspace. Nevertheless, the overall aim is to build a more secure cyberspace – “all within the context of maintaining the free and open nature of the Internet” [3, p. 35] and with deeper international cooperation [4, p. 50], [5]. Opposing the Western vision, Russia has engaged with cyberspace by adapting the idea of digital sovereignty through the development of Internet censorship and control. RuNet – the Russian segment of the Internet – is considered an extension of the existing territory in the Russian ‘information space’ and a promoter of a ‘digital Westphalia’ [2, p. 117]. In recent years, RuNet has become a platform for the Russian state to use its power by developing laws and technical solutions that challenge the idea of an open global Internet.

During the summer of 2016, almost simultaneously, as NATO recognised cyberspace as a military domain, Russia declared that RuNet would be disconnected from the global Internet by 2020 (‘RuNet 2020’). The contemporary global interpretation of cyber and information security stresses a tendency towards militarisation and the cyber arms race has begun [6], [4], [7], [5], [3]. It seems that both Western and Russian cyberspace and/or information space is becoming a new space for states to act and to reassert traditional notions of sovereignty – however through contradictory ‘open’ and ‘closed’ approaches.

Cyberspace experienced from within one state can radically differ from the cyberspace experienced from within another. In the Russian approach, cyberspace is used by ‘other countries’ and hostile forces for the destabilization of Russia [8], [9]. This kind of ‘besieged fortress’ mentality has characterised Russian thinking for decades. It follows the

[1] In this paper, ‘West’ (‘Western’) is defined as relating to the countries of EU and North America and their allies and used without quotation marks hereafter.

very same template repeatedly – the enemy is seen to be plotting to encircle Russia, invade, and overthrow the Russian political system [10, pp. 19, 36-39], [11, pp. 108-109] – by land, sea, air, or from space and now through cyberspace.

In this paper, I propose to look beyond Russia's 'self-victimisation' and try to see what is being done behind the 'external enemy' discourse. It seems that a number of Western scholars' view RuNet as 'pure propaganda' and do not seriously consider the possibility that the Russian segment of the Internet could be disconnected from the global Internet. Moreover, RuNet is not considered a threat to cybersecurity or even an instrument of deterrence. Nonetheless, in this paper, I am asking whether should 'RuNet 2020' be taken seriously and whether we are missing something fundamental about cybersecurity, because we observe cyberspace from our Western 'open and shared' viewpoint. The aim of this paper is to identify the essential contradictions in the views towards digital sovereignty and cybersecurity between Russia and the West. Moreover, the objective is also to attempt to understand the Russian way of thinking – and to be prepared for 'RuNet 2020'.

Firstly, this paper introduces Russian 'information space' and the concept of 'digital sovereignty'. Secondly, this paper provides a short introduction to RuNet and the Russian approach to cybersecurity. Thirdly, the measures that either have been done or aim to gradually isolate RuNet from the global Internet are listed. Finally as a conclusion, this paper provides a futuristic view of the global cyberspace of 2020 with or without RuNet.

Methodically this paper is a literature survey of writings pertaining to the Russian view of cybersecurity and information space. In the conceptual part of this paper, primary sources include the Russian Federation's information security doctrines and Ministries' statements. Secondary sources include Russian ICT specialists' commentary and academic educational material. Supporting material includes western commentary on Russian cyber/information terminology. The list of measures that aim to isolate RuNet is composed mainly of official press releases from Russian Ministries, newspaper articles and online materials from Russian news agencies. As an information or research source, Russian state-controlled media is challenging and the information given should be treated cautiously. However, it is the best up-to-date and open source information accessible, and since the original pieces are written in Russian, the material has been more or less targeted at the 'RuNet audience' rather than for purposes of international propaganda.

Additionally, supporting material has been collected from Western news agencies and academic studies. Critical reading and researcher positioning is important when using this type of data and writing a survey. It is always a subjective account of what is relevant. Therefore, this paper serves as an opening for discussion of 'situation awareness' of cyberspace and aims to indicate current and important themes for future studies on cybersecurity from a Russian studies perspective.

2 Does digital sovereignty ensure Russian information security?

The lack of common definitions for cyber terminology not only creates difficulties in mutual understanding, but also reflects a deeper problem – that there are fundamental differences in views about cybersecurity [12], [13]. The Russian understanding of 'cyberspace' is more comprehensive than in the West and therefore it is called 'information space' or 'information environment'. It can be defined as a sphere of human activity, related to creating, rendering and using information, ICT infrastructure and information itself [8], [9]. Russian information space includes all mass media, not only information and computer technology platforms [14, p. 14], [15, p. 7]. The Russian perspective highlights not only the technical wholeness of information but also the cognitive wholeness of information [13, p. 40]. Additionally, Russia's operational thinking divides information warfare into digital-technological (electronic warfare) and cognitive-psychological operations [16, pp. 244-245], [14, pp. 16-17]. Moreover, instead of the Western 'cybersecurity', 'information security' is used and is a much broader notion and is directly connected to the Russian state security [17, pp. 28-29], [14, p. 18]. Jaitner et al. [13, p. 40] argue that the use of non-Western terminology in Russian military strategies and doctrines is done deliberately. Similarly, Jolanta Darczewska [18, p. 10] claims that the Russian conceptualization has been intentionally developed in opposition to the Western cyber concepts, to create a certain kind of 'terminological newspeak' where – in Orwellian style – it is impossible to discuss the theme, because there are no concepts for it.

One example of such 'terminological newspeak' could be Russian *informatsionnoe protivoborstvo* (cf. [8], [9]) that is repeatedly and "deliberately" (cf. [19, p. 10]) incorrectly translated into English as 'information warfare'. However, in Russian *protivoborstvo* does not mean 'warfare', rather its literary translation would be 'counter struggle', 'counteraction' or 'countermeasure'. The verb *protivoborstvovat'* can be found in common dictionaries and is translated as ‘to oppose’ or ‘to fight against’ (New Comprehensive Russian – English Dictionary 2004 s.v. protivoborstvovat’). Whereas the verb ‘to counteract’ in English is explained rather similarly as ‘to act against or in opposition to’ or ‘to oppose’ (Oxford English Dictionary 2016 s.v. counteract). Thus, re-conceptualization might be appropriate and an improved translation for the ambiguous *informatsionnoe protivoborstvo* could be, for instance, ‘information countermeasure’ or ‘information counter struggle’. Unfortunately, the incorrect translation misses the intentionally created rhetorical game – as noted earlier – Russia has been ‘under attack’ for centuries. And for instance, in a cyber conflict situation Russia simply uses *informatsionnoe protivoborstvo*, i.e. ‘countermeasures’ – as a ‘defensive response’ to the eternal (Western) external enemy (cf. the Bronze soldier and cyber/information *protivoborstvo* on Estonia in 2007). According to Thomas [20, p. 574], simply overlapping Western concepts on Russian thinking does not always work. A better approach would be “to ponder how new concepts fit into Russia’s current military thought process” and this requires more intimate knowledge of Russia’s overall theoretical and planning processes [20, p. 574].

Digital sovereignty as a concept has been part of the Russian ‘information space’ discussion and research starting from 2012 [21, p. 125], [2, p. 113]. One of the main visionaries behind the concept is the innovator of RuNet and IT expert Igor Ashmanov, who has been envisioning digital sovereignty as the right and ability of the national government independently determine geopolitical national interests in the digital environment. When Ashmanov [22] speaks about ‘digital sovereignty’, he divides it into ‘electronic sovereignty’ that contains ‘cyber warfare sustainability’, and ‘information sovereignty’ that contains ‘information warfare sustainability’. According to Ashmanov’s definition, ‘electronic sovereignty’ represents a sustainable infrastructure providing protection from viruses, attacks, breaks, leakages, data theft, spam, etc. Whereas ‘information sovereignty’ is an independent control of information (filtering, blocking, distributing) and a resistance to information attacks (detection, prevention, counter-attack). According to Ashmanov, components of ideal digital sovereignty are autonomous hardware and software platforms (PC and network) and autonomous or controlled mobile platforms, autonomous internet infrastructure, autonomous mass media structures and TV, an autonomous system and means for propaganda and information warfare and sophisticated ideology with appropriate laws [22].

It seems Russia would want to treat ‘cyber’ as a geopolitical (or ‘geo-digital’) territory. Thus, digital sovereignty appears to be a logical concept for defining and safeguarding the borders of the Russian ‘information space’ and for ensuring ‘information security’. According to Ashmanov [22], the U.S is the only country in the world that has factual digital sovereignty. In the Russian approach, the Internet is a by-product of the dominant American culture and therefore, poses a threat to Russian cultural integrity and independence. The global Internet is dependent on popular applications and services that are provided by U.S. based companies, and therefore, pose a threat to Russian technological integrity and autonomy (cf. [9]). Moreover, the Internet is dominated by English and therefore, the Russian segment of the Internet – RuNet – has emerged as an alternative social universe that celebrates Russian cultural and intellectual traditions.

3 RuNet – from an alternative social universe to a model of a secure environment?

RuNet, i.e. the ‘Russian internet’ is a relatively closed online environment that is based on the Russian language. Nevertheless, RuNet refers not only to the Russian language, but also to the ‘Russian way’ of doing things (e.g. sovereignty, independence from the West, the ‘restoration’ of information sovereignty). RuNet is a self-contained environment with well-developed and highly popular research engines (*Yandex*, *Rambler*), social networking sites (*Vkontakte*, *Odnoklassniki*, *LiveJournal*, *Moi Mir*), and free e-mail services (*mail.ru*). RuNet has been generally defined as “a totality of information, communications and activities which occur on the Internet, mostly in the Russian language, no matter where resources and users are physically located, and which are somehow linked to Russian culture and Russian cultural identity” [23, p. 27].

At the beginning, RuNet developed largely free from state influence [23]. However, for the past few years, the Russian government has been significantly tightening the control of the Russian information space. The increasing activity of the government makes RuNet not only ‘more Russian’ but also more state-affiliated – the state controls the Internet within its borders and censors or suppresses the information circulated in the Russian information space. Therefore, today RuNet offers new perspectives for governing the country. In addition, RuNet offers a ‘sphere of influence’ or ‘near abroad’ type of channel in digital form (e.g. influencing the Russian speaking minority in Finland). Furthermore, the increasing ‘closed, safe and secure’ rhetoric encourages Russian Internet users to stay within the framework of the ‘national web’ and this shaping of the information space gives rise to a natural and self-attained isolation. In a global context, RuNet could be seen as a certain kind of prototype for the development of ‘digital sovereignty’. RuNet diminishes the value of the Western ‘free and open’ Internet – facilitates further digital balkanization and encourages the emergence of other ‘sovereign Internets’. Consequently, RuNet has evolved from an alternative social universe to a state-controlled ‘safe and secure’ digital environment manifesting ‘digital sovereignty’.

4 Russian measures towards digital sovereignty

In the Russian press in May 2016, the Russian Ministry of Communications (*Minkomsvyaz*) circulated new additions to the state ‘Information Society’ [24] programme that ensures the protection of the critical Russian Internet infrastructure. The updated programme includes plans to eliminate the dependence of RuNet on external networks and to ensure that RuNet will be fully controlled by the state. *Minkomsvyaz* declared that by 2020, 99% of Russian Internet traffic should be transmitted within the country and that it is going to create a ‘back-up-copy’ of 99% of the ‘critical infrastructure’ within Russia. At that point, the ‘critical infrastructure’ was not defined [25].

In the recent Information Security Doctrine signed by Vladimir Putin on December 5, 2016, Russia openly aims “to deploy a national system of managing the Russian segment of the Internet” [9]. This statement is not elaborated in the document. However, there are factual measures that resonate well with the new doctrine. These measures either have been implemented already or aim at to gradually isolate RuNet from the global Internet infrastructure. Thus, in the following is presented a list of Russian linguistic, cultural, legislative, economic, military and technical measures towards digital sovereignty.

4.1 Language, culture and spirituality

Today Russian is the second most used language on the Internet and the number of users of RuNet is considered the largest in Europe [6, p. 22]. For years Russians had been demanding ICANN (The Internet Corporation for Assigned Names and Numbers) to break the English language dominance of Internet. The Cyrillic domain battle was aimed at raising the status of Russian as a global language, and it was hoped to expand Internet use among Russian speakers unfamiliar with Latin characters [26, p. 190]. The first internet domains using the Cyrillic script were launched on May 13, 2010 after Russia was officially assigned the .рф (.rf, for "Russian Federation") domain. Currently Russia has three different domain types: .ru, .su, and .рф (.su stands for Soviet Union). At the same time, national domains in Arabic were also given to Egypt, the United Arab Emirates and Saudi Arabia.

According to the Information Security Doctrine [9], "increased information influence on the population of Russia, mainly on the young generation, aimed at eroding traditional Russian spiritual and moral values" proposes a serious threat to Russian information security. A project called 'The Clean Internet' endorsed by *Minkomsvyaz* in 2012, serves as an example of the shaping of the Russian information space and its natural and self-attained isolation. Within this project a voluntary association called the 'Safe Internet League'[2], that celebrates the 'closed, safe and secure' rhetoric, was established [27, p. 298]. According to its website, the Safe Internet League is the largest and most reputable Russian organisation fighting dangerous Web content. Its volunteers monitor the Internet for violations on behalf of law enforcement. In the league's view, violations include child pornography, pornography accessible to children, promotion of drug and alcohol abuse, as well violent or 'extremist' content. Despite the prominent role assigned to countering child pornography, the league's actual focus is social media. In many people's opinions, the league in fact acts as an attempt by Russia's law enforcement to monitor social media's expansion [26, pp. 189-190], [27, pp. 201-202].

4.2 Legislation for surveillance and control

Russia has intensively ratified new laws that support the Information Security Doctrine's objectives. Between 2012 and 2014, the Russian government passed eight laws that aimed at gaining a complete control over RuNet [28], [29, p. 175]. Moreover, some of these laws have already been tightened during 2015-2016. These laws allow, for instance, *Roskomnadzor* to block and to censor harmful information and websites deemed extremist or a threat to public order; demand the owners and operators of websites to store all information about the arrival, transmission, delivery, and processing of voice data, written text, images,

[2] http://www.ligainternet.ru/en/

sounds, or other kinds of action and to keep this content for six months. The laws further limit anonymous money transfers and donations on the Internet and require all web-based writers (bloggers, social media accounts) with posts that exceed 3,000 page-views to register with the government. They also aim to curb the dissemination or re-dissemination (tweeting and retweeting) of ‘extremist materials’ and require Internet companies, including Google, Twitter, and Facebook, to locate servers handling Russian Internet traffic inside the country and to store their users’ data on these locally based servers for a minimum of six months. Furthermore, these laws prohibit anonymous access to the Internet in public spaces. Moreover, some of these laws have already been tightened during 2015-2016 [27, pp. 215-216; 263-264], [29, p. 176].

In October 2016, *Minkomsvyaz* released a new draft bill that defines basic Internet infrastructure concepts such as ‘autonomous system’ and ‘infrastructure of the Russian national segment of the Internet’ and ‘national .ru and .рф zone domain name registrar’ from the Russian point of view. The ‘Russian national segment of the Internet’ is defined as the infrastructure that enables the assigning and functioning of country-code domain names (domain names that end in .ru and .рф), systems that can manage the flows of Internet traffic, and other fundamental Internet communication hardware [25].

The draft bill mandates that the state would control the RuNet’s entire ‘critical infrastructure’, including the national .ru and .рф domains, traffic exchange points, as well as autonomous systems and networks belonging to various corporations and individuals, i.e. it forces all domains in the .ru zone to be hosted in Russia. Here for the first time ‘critical infrastructure’ is defined in detail. This information resonates with earlier statements by *Minkomsvyaz* who claimed Russia was in need of its own reserve systems should its Internet segment be ‘cut off’ from the rest of the world if Russia faces a ‘national emergency’ such as ‘military action’ or ‘serious protest actions’ [25], [30], [29, p. 175]. In January 2017 a new bill passed titled “On the Security of Critical Infrastructure of the Russian Federation” that mandates the formation of a special register of all companies and agencies that control objects of critical infrastructure [31]. It seems that all of the RuNet’s critical infrastructure will fall under complete control of the Russian state authorities and a new official state register of IP addresses for RuNet may appear.

4.3 Domestic software

The Information Security Doctrine [9] calls for eliminating the dependence of domestic industries on foreign information technologies and ensuring information security by developing effective Russian technologies. In 2011, the intention was to develop a ‘national operating system’ that would reduce the Russian dependency on Microsoft Windows. Yet the project was called off in 2012 when Nikolai Nikiforov was appointed as the head of the Ministry of Communications. Since then, Nikiforov has repeatedly stated that Russia does not deed a national operating system. Rather he would promote a ‘BRICS operating system’ [32]. In September 2016, it was reported that the city of Moscow would replace Microsoft programmes with domestic software on thousands of computers. Furthermore, State media company *Rossiya Segodnya* and Moscow’s regional government switched from Oracle database systems to open-source-software (PostgreSQL) maintained by local programmers [33], [34].

In October 2016, it was declared that the Russian ‘military Internet’ (*voennyi internet*) was fully operational. Officially, the system is referred to as the ‘closed segment for data transmission’ and it is not connected to the global Internet and all the computers connected to it rely on domestic components and software [35]. What makes the military Internet interesting is that it is supposed to have an e-mail system for transferring highly classified information, including ‘top secret’ documents that would make it the fastest way to transfer information in a combat situation. Moreover, the closed military Internet is a response to the concern that the Russian armed forces’ and other state institutions’ information security is threatened by foreign intelligence agencies [9]. Consequently, the closed military Internet could serve as a testing ground for domestic hardware and software and manifests independence from the West.

The need for domestic solutions in the economic sphere is also underlined in the Information Security Doctrine [9]. The necessity for having a Russian domestic SWIFT and a national payment system became more acute after sanctions were imposed against Russia after the Crimea takeover and war in Eastern Ukraine in 2014. In January 2016, it was reported that about a half of the Russian banks have turned to using the domestic equivalent to SWIFT [36]. A national payment system would enable independence from the West and could be used together with new allies, for instance, the BRICS countries.

4.4 The BRICS cable and new non-western allies

The BRICS countries – Brazil, Russia, India, China, and South Africa – aim together to challenge the hegemony of the U.S. in global affairs. In 2013, BRICS decided to build their own internet infrastructure 'hidden from NSA' – to enhance cybersecurity and to create a parallel cyber universe. It was announced that they would connect the BRICS counties with a new high-capacity underwater cable that goes from Brazil, around the Cape of Good Hope, northeast up to India, along the Chinese coast and up to Vladivostok in eastern Russia. The length of the fibre-optic cable would be over 33 thousand kilometres, making it one of the most ambitious underwater telecoms projects ever attempted. The main goal of the project is to create sovereign data accesses, bypassing all parts of Internet infrastructure located outside BRICS countries. Russia sees BRICS as an influential global actor with 'its own voice' on cybersecurity issues [2], [37].

4.5 RuNet as a 'back-up-copy' – technical plans of 2016

It has been reported that the Russian authorities (*Minkomsvyaz*, *Roskomnadzor*, Ministry of Defence, FSB and Rostelekom) carried out exercises in disconnecting RuNet from the global infrastructure in 2014. Also, it has been stated that during the exercise *Roskomnadzor* ordered communications hubs run by the main Russian Internet providers to block traffic to foreign communication channels by using a traffic control system called Deep Packet Inspection (DPI). However, the experiment failed because thousands of smaller service providers, which *Roskomnadzor* had little control over, continued to pass information out of the country [38]. In addition, Russian officials originally initiated the idea of creating and maintaining a 'back-up-copy' of RuNet in 2014 [39], [40], [41].

Together with the additions to the 'Information Society' state programme launched in June 2016, more detailed technical plans for disconnecting RuNet from the global Internet by 2020 were also announced. According to the Russian news agencies, an autonomous non-commercial organization MSK-IX, which owns, along with Rostelekom, the largest traffic exchange point in Russia, started to study the formation of 'back-ups' of the RuNet [39], [40], [41]. The terms for 'back-up' mostly used in Russian are *rezervnaia (kopiia)* (reserve, spare or back-up), *dubl'* (from English word 'double') and more rarely *zerkalo* (a mirror).

According to Alexey Platonov, head of MSK-IX, in the first phase they will conduct macroscopic studies of the Internet that will be identified as ‘walking’ traffic and interaction between autonomous systems. Their study will form the basis of a unified system that will combine the databases of the Dutch RIPE NCC, which is responsible for distributing IP addresses between telecommunications operators, including Russian, and other registries and databases of Internet route information, i.e. the intention is to make an analogue of RIPE [39]. Now each operator independently determines the policy for routing traffic. Companies do not share this information with each other, but manifest their routes in the routing database — the Internet Routing Registry, which is also under the control of the RIPE NCC [40].

Minkomsviaz also intends to create its own set register of traffic exchange points and to oblige operators to use only registered points. It will be proposed to holders of these points to build reserve channels of communication funded from the state budget. Only operators, who have a license for cross-border data communication, may organise international communication channels. Such international communication is not under control of SORM, which must be installed by each Russian operator [39], [40]. All these proposed technical measures aim to control the Internet routing architecture inside Russia and to be prepared for maintaining operational capabilities outside the global Internet.

5 Discussion – A global cyberspace of 2020 with or without RuNet

The aim of this paper has been to illustrate to the Western audience the nature of Russian information space and digital sovereignty and to understand the Russian way of thinking about information security and/or cybersecurity. As shown in this paper, the Western idealism of having an ‘open, safe and secure’ Internet has been seriously challenged by ‘closed, safe and secure’ Russian alarmism. It seems that Western scholars have largely underestimated measures that Russia has achieved mentally, legally and technically in creating RuNet. RuNet is not considered a threat to cybersecurity or even an instrument of deterrence in the West. Observing Russia through Western concepts, prevents us to comprehend how strong the ‘renewal’ of the information sovereignty concept truly is and how goal-oriented Russia is and how rapidly she is heading towards ‘digital sovereignty’. The Russian challenge to the US-dominated/led world order is real, serious and long-term [10, pp. 19, 36-39], [11, pp. 108-109]. It is tempting to perceive the Russian government's Internet policy as backward and authoritarian. However, the 'official Russia' strongly believes in and endorses the endeavour that the Russian segment of the Internet will be technically disconnected from the global Internet by 2020. The ambition is to control the Internet routing architecture inside Russia and to maintain operational capabilities outside the global Internet. Consequently, the isolation of RuNet would have at least three alarming and potentially serious outcomes from the cybersecurity point of view: 1) "Weaponization of information"[3]; 2) Fragmentation of the global Internet; 3) Intensification of cyber deterrence; of which the first two have been more or less already been realized.

In an isolated RuNet, it will be even more difficult to confront Russia's "weaponization of information". We should expect coordinated information operations targeted both at 'domestic' audiences and the 'near abroad' audience to convince them they are under attack and thus justify greater censorship of RuNet. RuNet will keep opposing information out and Russian data in for security purposes. Moreover, information warfare targeted outside RuNet will be easier to conduct and the recruitment of free-will agitators ('information fighters') will occur almost naturally. After the US presidential elections of 2016, there has been a growing concern about Russia's intentions to exert covert influence over peoples and governments.

Furthermore, RuNet might serve as an example and encourage the emergence of other 'sovereign internets' and push global cyberspace towards fragmentation. There are already several examples of aims to 'de-Westernize' and maintain control over Internet users and control the spread of information, e.g. the Great Firewall of China, the Halal Internet of Iran, Pakistan's intranet, the BRICS Internet, and data localization requirements etc. 'De-westernizing' and digital balkanization would influence cybersecurity fundamentally.

Information space is still relatively new to the Russian military. However, Russia is intensely developing both its defensive and offensive capabilities to operate in the cyber realm. It seems that Russia is preparing itself for a confrontation in a hostile environment [9]. Clearly, Russia has

[3] The concept "Weaponization of information" was first used by Pomerantsev et al [48].

integrated offensive cyber capabilities, including DDos-attacks, malware, and advanced information warfare (e.g. troops for 'informational operations') into its military arsenal. The arms race in cyberspace is certainly accelerating. We in the West no longer ask 'if' an attack on our network will be successful, but 'where' and 'how' it will occur [5]. However, perhaps this is what Russia wants us to contemplate when it is by itself focused on building resilience on a national level and aiming towards digital sovereignty. The 'RuNet 2020' project indicates that Russia is not competing in terms of 'cyber weapons' or 'cyber-attack capabilities', but on 'resilience' and 'recovery plans'. In this arms race, Russia is leading and as a result, Russia might be writing a new chapter in the theory of cyber deterrence.

There is a great deal of confusion about how deterrence would work in the cyber domain. The new Russian Information Doctrine states that strategic deterrence and preventing military conflicts are among the main reasons for ensuring information security [9]. Nevertheless, applying classical Cold War deterrence theory to cyber warfare is disputable and still very much in process [42], [43], [44], [45], [46]. Moreover, the Russian 'strategic deterrence' (*strategicheskoe sderzhivanie*) concept is broader than the direct Western equivalent. It contains defensive, nuclear, non-nuclear and non-military deterrent tools [47]. Simply, the success of deterrence comes down to the ability to convince others that there is no point in attacking. If Russians are able to develop an independent and resilient network that can absorb an attack, limit its impact as much as possible, and be quickly restored to full operational capability, it could serve as a new form of cyber deterrence that can be referred to as 'deterrence by denial' [46, p. 38] or 'dissuasion by denial' [43, p. 353]. 'Deterrence by denial' in the RuNet context would mean persuading the enemy not to attack by convincing him that his attack will be defeated. This could fall under the non-military deterrence component of the Russian strategic deterrence concept [47, pp. 14-15]. Moreover, Russia could deter to attack both technically and kinetically on the global network when their own system is not dependent on it.

In the Western mind-set, 'deterrence by denial' has been recognised as 'answer to cyberattack' [46, p. 38]. However, it has been considered too difficult to achieve "without major technical advances and significant new policies" [46, p. 39]. As shown in this paper, Russia has very intensively developed domestic hardware and software, pursued alternative technical solutions and ratified new laws and policies. In the Russian understanding, a technically independent and legally supported RuNet will be a safe and reliable digital infrastructure. Thus, 'RuNet 2020' could be considered as a Russian ‘disaster recovery plan’ and ‘business continuity plan’ that EU countries have only recently started to consider and plan for [5].

Once RuNet is technically successful, Russia will raise its level of cyber resilience to a new level – it will claim digital sovereignty and the era of the global Internet may appear to be passing. Russia’s prospective digital sovereignty will be pursued through a combination of propaganda, psychological operations and manipulation of information. Before this occurs, it is important to understand the context in which Russia makes its assessments. We should re-conceptualise, obtain knowledge of the planning processes and re-analyse Russian ‘information space’ comprehensively. Certainly, ‘RuNet 2020’ should be taken seriously.

References

[1] T. Tuukkanen, “Sovereinty in the cyber domain,” in *The Fog of Cyber Defence*, J. Rantapelkonen and M. Salminen, Eds., Helsinki, National Defence University, 2013, pp. 37-45.

[2] J. Nocetti, “Contest and conquest: Russia and global internet governance,” *International Affairs,* vol. 91, no. 1, pp. 111-130, 2015.

[3] National Cyber Security Strategy, 2016. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. [Accessed 18 November 2016].

[4] J. Limnell, “The cyber arms race is accelerating – what are the consequences?,” *Journal of Cyber Policy,* vol. 1, no. 1, pp. 50-60, 2016.

[5] “EU concept on Cyber Defence for EU-led Military Operations and Missions,” 2016.

[6] E. Zinovieva, “Vozmoshnosti Rossii v global’nom informatsionnom obshchestve [Russia in the global information society],” *Vestnik MGIMO universiteta / MGIMO Review of International Relations,* vol. 48, no. 3, pp. 17-29, 2016.

[7] Nato Cyber Defence Fact Sheet, July 2016. [Online]. Available: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf. [Accessed 18 October 2016].

[8] "Doktrina informatsionnoi bezopasnosti Rossiiskoi Fereratsii [Information Security Doctrine of the Russian Fereration]," 9 September 2000. [Online]. Available: http://www.scrf.gov.ru/documents/6/5.html. [Accessed 1 Mach 2017].

[9] "Doktrina informatsionnoi bezopasnosti Rossiiskoi Fereratsii [Information Security Doctrine of the Russian Fereration]," 5 December 2016. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. [Accessed 27 December 2016].

[10] D. Trenin, Should We Fear Russia?, Cambridge: Polity Press, 2016.

[11] M. Heller, Cogs in the Wheel: The Formation of Soviet Man, London: Collins Harvill, 1988.

[12] G. Giles, Handbook of Russian Information Warfare, vol. Fellowship Monograph 9, Naro Defence College, 2016.

[13] M. Jatner and P. Mattsson, "Russian Information Warfare of 2014," in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn, 2015.

[14] S. Makarenko and I. Chucklyaev, "Termonologicheskii basis v oblasti informatsionnogo protivoborstva [The terminological basis of the informational conflict area]," *Voprosy kiberbezopasnosti,* no. 1, pp. 13-21, 2014.

[15] Y. Kabanov, "Information (Cyber-) Security Discourses and Policies in The European Union and Russia: A Comparative Analysis," 2014. [Online]. Available: http://www.zdes.spbu.ru/assets/files/wp/2014/WP_2014_1%20%20Kabanov.compressed.pdf. [Accessed 31 November 2016].

[16] I. Panarin and L. Panarina, Informatsionnaia voina i mir. Informatsionnoe protivoborstvo v sovremennom mire [Information War and Peace. Information Counter Struggle in the Contemporary World], Moskva: OLMA-PRESS, 2003.

[17] D. Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," November 2015. [Online]. Available: http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf. [Accessed 2 March 2017].

[18] J. Darczevska, "The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study," 2014. [Online]. Available: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf. [Accessed 1 March 2017].

[19] U. Franke, “War by non-Military Means: Understanding Russian Information Warfare. FOI-R-4065-SE,” 2015. [Online]. Available: https://pdfs.semanticscholar.org/2869/71ba9762da1d039d0d40a27c94e0ec8d31ac.pdf. [Accessed 18 October 2016].

[20] T. Thomas, “The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking,” *Journal of Slavic Military Studies,* vol. 29, no. 4, pp. 554-575, 2016.

[21] D. Dubov, “Kibermogushchestvo kak bazis obespecheniia ”tsifrovogo” suvereniteta v sovremennom mire: kliuchevie podkhody. [Cyberpower as a fundamental concept for “digital” sovereignty in the contemporary world: Key aspects],” *Oborona i bezopasnost',* vol. 4, no. 25, pp. 123-135, 2014.

[22] I. Ashmanov, "Doklad: Informatsionnyi suverenitet. Sovremennaia real’nost’, [Presentation: Information Sovereignty. Contemporary Reality]," 24 April 2013. [Online]. Available: http://rossiyanavsegda.ru/read/948/. [Accessed 17 October 2016].

[23] E. Gorny, A Creative History of the Russian Internet. Studies in Internet Creativity., Berlin: DVM Verlag Dr. Muller, 2009.

[24] Minkomsviaz, “Gosudarstvennaia programma ”Informatsionnoe obshchestvo” (2011-2020 gody), [State program “Information Society” (2011-2020)],” 27 August 2014. [Online]. Available: http://minsvyaz.ru/ru/activity/programs/1/ . [Accessed 2016 October 2016].

[25] Minkomsvyaz, “Federal’nyi zakon “O vnesenii izmenenii v Federal’nyi zakon “O sviazi” (Proekt) [Federal Law “On the changes to the Federal Law “On connections”],” 11 October 2016. [Online]. Available: http://regulation.gov.ru/projects#npa=58851. [Accessed 22 October 2016].

[26] M. Gorham, After Newspeak: Language, Culture and Politics in Russia from Gorbachev to Putin, New York: Cornell University Press, 2014.

[27] A. Soldatov and I. Boroganov, The Red Web: The Struggle between Russia’s Digital Dictators and the New Online Revolutionaries., New York: PublicAffirs, 2015.

[28] J. Nocetti, ”Russia’s ‘dictatorship-of-the-law” approach to internet policy.,” *Internet Policy Review. Journal on Internet Regulation,* osa/vuosik. 4, nro 4, pp. 1-19, 2015.

[29] P. Vargas-Leon, “Tracking Internet Shutdown Practices: Democracies and Hybrid Regimes,” in *The Turn to Infrastructure in Internet Governance*, New York, Palgrave Macmillan, 2016, pp. 167-188.

[30] A. Golitsyna and A. Prokolenko, “Chnovniki khotiat podchinit’ sebe ves’ rossiiskii internet [Officials want to supress the entire Russian Internet under their control],” 27 May 2016. [Online]. Available: http://www.vedomosti.ru/technology/articles/2016/05/27/642739-chinovniki-hotyat-internetom. [Accessed 2 November 2016].

[31] "Zakonoproekt No. 47571-7: "O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii" [Bill No. 47571-7: "On the Security of Critical Infrastructure of the Russian Federation]," 2017. [Online]. Available: http://asozd2.duma.gov.ru/addwork/scans.nsf/ID/EBE024490F4C58514325808100054D3AC/$File/47571-7_06122016_47571-7.PDF?OpenElement . [Accessed 6 March 2017].

[32] “Polnaia videozapis’ repliki Nikolaia Nikiforofa na ”Gaidarovskom Forume 2016”, [Full video clip of Nikolai Nikiforov’s statement at the Gaidar ”Forum 2016”],” 16 January 2016. [Online]. Available: https://vk.com/video292653561_171817033. [Accessed 22 October 2016].

[33] I. Khrennikov, ”Moscow Drops Microsoft on Putin’s Call for Self-Sufficiency,” 27 September 2016. [Online]. Available: https://www.bloomberg.com/news/articles/2016-09-27/moscow-drops-microsoft-outlook-as-putin-urges-self-sufficiency. [Haettu 30 September 2016].

[34] T. Kostyleva, “Uchastniki IT-rynka ob importozameshchenii softa: zakon slishkom miagkhii, o rezul’tatakh govorit’ rano. [Participants of the IT-development on the software substitution: The law is too soft, it is too early to speak about results],” 23 September 2016. [Online]. Available: http://d-russia.ru/uchastniki-it-rynka-ob-importozameshhenii-softa-zakon-slishkom-myagkij-o-rezultatax-govorit-rano.html. [Accessed 30 September 2016].

[35] V. Zykov ja A. Ramm, ”V Rossii poiavilsia voennyi internet [A military Internet has appeared in Russia],” *Izvestiia,* 19 October 2016.

[36] A. Alekseevskikh, “Rossiiskie banki zashchitilis’ ot otkliuchenii iz Briusselia [Russian banks Russian banks protect themselves against outages from Brussels],” *Izvestiia,* 11 January 2016.

[37] A. Gupta, “Cold War-Style ‘Cyber Arms Race’ between US and Russia: Reality or Rhetoric? 98/16,” Center for Air Power Studies, 2016.

[38] R. Oliphant, ”Russia 'tried to cut off' World Wide Web,” 15 October 2015. [Online]. Available: http://www.telegraph.co.uk/news/worldnews/europe/russia/11934411/Russia-tried-to-cut-off-World-Wide-Web.html. [Haettu 19 October 2016].

[39] A. Sukharevskaia, "Zapasnoi internet: Kto zaimetsia sozdaniem ”reservnoi kopii” [Spare Internet: Who Will Establish the “Back-Up-Copy”]," *RBK: ezhednevnaia delovaia gazeta,* 7 July 2016.

[40] A. Sukharevskaia and I. Iuzbekova, "Tri voprosa o suverennom runete [Three Questions about Sovereign RuNet]," *RBK: Ezhednevnaia delovaia gazeta,* 6 June 2016.

[41] D. Nazarov, "Rezervnaia kopiia: Mozhno li otkliuchit’ rossiiskii internet ot global’noi seti? [Back-Up-Copy: Can the Russian Segment of the Internet be Disconnected from the Global System?]," 1 September 2016. [Online]. Available: http://www.furfur.me/furfur/freedom/freedom/218695-chto-takoe-rezervnaya-kopiya-interneta. [Accessed 4 October 2016].

[42] A. Bendiek and T. Metzger, “Deterrence theory in the cyber-century, Working Paper, Research Division EU/Europe Stiftung Wissenschaft und Politic, German Institute for International and Security Affairs,” 2015. [Online]. Available: https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf . [Accessed 15 November 2016].

[43] P. Davis, “Toward theory for dissuasion (or deterrence) by denial: using simple cognitive models of the adversary to inform strategy, RAND Working Papers, WR-1027,” January 2014. [Online]. Available: http://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1027/RAND_WR1027.pdf . [Accessed 1 December 2016].

[44] J. Lindsay, “Tipping the scales: the attribution problem and feasibility of deterrence against cyberattack,” *Journal of Cybersecurity,* vol. 1, no. 1, pp. 53-67, 2015.

[45] T. Stevens, “A cyberwar of ideas? Deterrence and norms in cyberspace,” *Contemporary Security Policy,* vol. 33, no. 1, pp. 148-170, 2012.

[46] D. Elliot, “Deterring strategic cyberattack,” *IEEE Security and Privacy,* vol. September/October, pp. 36-40, 2011.

[47] K. Bruusgaard, “Russian strategic deterrence,” *Survival,* vol. 58, no. 4, pp. 7-26, 2016.

[48] P. Pomerantsev and M. Weiss, “The meanence of unreality: How the Kremlin weaponizes information, culture and money,” 2014. [Online]. Available: http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf. [Accessed 15 November 2016].

‘RuNet 2020’ – Deploying traditional elements of combat power in cyberspace?

Juha-Pekka Nikkarila & Mari Ristolainen

Abstract

In the recently approved Information Security Doctrine (Dec 5, 2016) Russia openly aims “to deploy a national system of managing the Russian segment of the Internet”. For some time, we have observed how Russia has been conducting intellectual, legislative and technical measures to create a purely domestic network disconnected from the global Internet by 2020. In the Russian way of thinking, a fully state-controlled and independent RuNet – the Russian segment of the internet – will ensure stronger defence against external attacks. In this paper, we play with the idea that RuNet will be disconnected technically from the global Internet by controlling the Internet routing architecture inside Russia and that Russia will be able to maintain operational capabilities outside the global Internet. Our aim is to discover what Russia’s military aim with ‘RuNet 2020’ could be. We argue that the strategy behind ‘RuNet 2020’ can be analysed with conventional military tactics and by the deployment of traditional elements of combat power in abstract cyberspace. We discuss that the military aim of ‘RuNet 2020’ is not the evident protection improvement, but to improve relative manoeuvrability. Moreover, ‘RuNet 2020’ could increase relative firepower as well. Consequently, our aim is to show how and why the Russian leadership could rely on ‘RuNet 2020’.

Keywords: Cyber defence, military tactics, elements of combat power, cyberspace as a military domain, cyber situation awareness, RuNet, Russia, Russian Information Security Doctrine

The first version of this paper has been published and presented at the International Conference on Military Communications and Information Systems (ICMCIS 2017), Oulu, Finland, May 15-16, 2017.

1 Introduction

During the past years, we have observed how Russia has implemented novel ways of conducting confrontation by combining conventional and unorthodox means of traditional warfare [1]. It seems that the Russian military and security mentality differs substantially from the 'Western'[1] approaches. Likewise, Russian understanding of 'cyberspace' is more comprehensive and therefore it is called 'information space' or the 'information environment'. Russian information space includes all mass media, not only information and computer technology platforms [2, pp. 1, 2a-h][2]. Moreover, Russia's military operational thinking divides 'information warfare' into digital-technological and cognitive-psychological operations [3], whereas in the 'West' we tend to speak separately about 'cyberwarfare' (digital-technological operations) and 'information warfare' (cognitive-psychological operations). In this paper we use the term 'information' in the way Russians perceive it.

During the summer of 2016, almost simultaneously, as NATO recognized cyberspace as a military domain, Russia declared that RuNet – the Russian segment of the Internet – would be disconnected from the global Internet by 2020. In the recent Information Security Doctrine signed by Vladimir Putin on December 5, 2016, Russia openly aims "to deploy a national system of managing the Russian segment of the Internet" [2, p. 29e]. In the Russian approach, the Internet is a by-product of the dominant American culture and the free flow of information poses a threat to Russian cultural integrity and independence. For some time, we have observed how Russia has been conducting intellectual, legislative and technical measures to create a purely domestic network [4]. In the Russian way of thinking, a fully state-controlled and independent network will ensure stronger defence against external attacks. Furthermore, Vladimir Putin's advisor German Klimenko, stated that Russia must be prepared to be disconnected from the global Internet because of the high probability of "tectonic shifts in the direction of deterioration" in relations with the West [5]. It seems that Russia is developing both defensive and offensive cyber capabilities to prepare itself for a confrontation in a hostile environment [2]. Hence, the 'RuNet 2020' project differs from the majority of efforts (e.g. by India, Pakistan, Cuba, Iran, and North-Korea) to control Internet traffic because it aims towards a 'digital sovereignty'

[1] In this paper, 'West' ('Western') is defined as relating to the countries of EU and North America and their allies and used without quotation marks hereafter.

[2] The numbers given refer to the Doctrine's section numbers and the letters in the Latin alphabet refer to the order not to page numbers.

and attempts to have a role in national defence and warfare in general as well. China and Russia already cooperate in the field of digital sovereignty. [6] Russian 'information security' is directly connected to the Russian state security [2, p. 30] [7]. Therefore, it is essential to analyse 'RuNet 2020' also in the context of military tactics.

It is tempting to perceive 'RuNet 2020' as a rather 'utopian project' and to dismiss the Russian government's Internet policies as backward and authoritarian. Yet, diverse national agendas and levels of technology lead to different prioritisations in cyber and/or information security that we should also take into consideration in national cyber defence strategies [8]. Hence, in this paper we play with the thought that the Russian segment of the Internet will be disconnected technically from the global Internet by controlling the Internet routing architecture inside Russia and that Russia will be able to maintain operational capabilities outside the global Internet. Our objective is to discover what Russia's military aim with 'RuNet 2020' could be. We argue that the strategy behind 'RuNet 2020' can be analysed with conventional military tactics and the deployment of traditional elements of combat power in the abstract cyber military domain. We wonder if the Russian 'new type of thinking' and 'information warfare strategy' is to 'unorthodoxly' (or 'creatively') integrate 'old-generation warfare' (cf. 'new generation warfare') into cyberspace. Consequently, our aim is to show how and why the Russian leadership could rely on 'RuNet 2020'.

Firstly, this paper introduces the conceptual and technical ideas behind 'RuNet 2020' and reads the Information Security Doctrine between the lines. Secondly, the traditional military tactics and basic combat elements are presented. Thirdly, 'RuNet 2020' is analysed from a conventional military tactics perspective via the traditional elements of combat power. Finally, the results are presented in a game theoretical model and the outcomes are discussed from the global cyber defence point of view. This highly topical paper offers a fresh multidisciplinary approach to cyber defence studies. It brings new knowledge, and potential measures for cyber situation awareness and security metrics; including cyber defence simulation and training.

2 Methods and materials

In this paper, we combine methods and materials from Russian and military studies. The conceptual and technical background is a literature survey explaining the ideas and measures behind 'RuNet 2020'. Military tactics and traditional elements of combat power are specified in an exploratory examination of theoretical military literature to name the basic common concepts that could be applicable in the cyber military domain. This examination forms a conceptual basis for the analysis of the military aim of ‘RuNet 2020’, the consequences of which are presented in a game theoretical model which is suitable for visualising the possible different paths if Russia is able to deploy RuNet and disconnect all its networks from the Internet. A context analysis of the Information Security Doctrine [2] and the Military Doctrine [9] of the Russian Federation is used for justifying and supporting the model.

The primary research material consists of the Information Security Doctrine [2] and the Military Doctrine [9] of the Russian Federation. Secondary sources include presidential speeches, ministries’ official press releases, newspaper articles and online materials from Russian news agencies. Theoretical literature and academic papers in the field of military tactics, cyber defence and Russian military thinking are further used as supporting material.

3 Conceptual background of ‘RuNet 2020’

The RuNet, i.e. the ‘Russian internet’ is a relatively closed online environment that is based on the Russian language. Nevertheless, RuNet refers not only to the Russian language, but also to the ‘Russian way’ of doing things. Generally, RuNet is a self-contained environment with well-developed and highly popular search engines, social networking sites, and free e-mail services. Likewise, the rights of Russian speakers unfamiliar with Latin characters have been consciously fought for. After a long debate, Russia was officially assigned the Cyrillic domain .рф (.rf, for ‘Russian Federation’) in 2010 [10, p. 190]. Currently Russia has three different domain types: .ru, .su, and .рф (.su stands for Soviet Union) and Russian is the second most used language on the Internet and the number of users of RuNet is considered the largest in Europe [11, p. 22].

3.1 Digital Sovereignty

At the beginning, RuNet was developed largely free from state influence [12]. However, for the past few years, the Russian government has been significantly tightening the control of the Russian information space. The increasing activity of the government makes RuNet not only ‘more Russian’ but also more state-affiliated – the state controls the Internet within its borders and censors or suppresses information circulated in the

Russian information space. In a global context, ‘RuNet 2020’ could be seen as a certain kind of prototype for the development of ‘digital sovereignty’ [4]. In the Russian approach, ‘digital sovereignty’ is envisioned as the right and ability of the national government to independently determine geopolitical national interests in the digital environment [13] [4].

3.2 Critical Infrastructure

In May 2016, the Russian Ministry of Communications (*Minkomsvyaz*) announced plans to ensure the protection of Russian ‘critical infrastructure’. The aim was to eliminate the dependence of RuNet on external networks and to ensure that RuNet would be fully controlled by the state. *Minkomsvyaz* declared that by 2020, 99% of Russian Internet traffic should be transmitted within the country and that the government is going to create a ‘back-up-copy’ of 99% of the ‘critical infrastructure’ within Russia [14]. In October 2016, *Minkomsvyaz* released a draft bill that would enable government agencies to have exclusive rights for contracting the national domain administrator and Internet providers to keep RuNet running, among other things [14]. The draft bill defines basic Internet infrastructure concepts such as ‘autonomous system’ and ‘infrastructure of the Russian national segment of the Internet’ and ‘national .ru and .рф zone domain name registrar’ from the Russian point of view. In addition, the ‘Russian national segment of the Internet’ is defined as the infrastructure that enables the assigning and functioning of country-code domain names (domain names that end in .ru and .рф), systems that manage the flows of Internet traffic, and other fundamental Internet communication hardware [14]. The draft bill mandates that the state would control the RuNet’s entire ‘critical infrastructure’, including the national .ru and .рф domains, traffic exchange points, as well as autonomous systems and networks belonging to various corporations and individuals, i.e. it forces all domains in the .ru zone to be hosted in Russia. Here for the first time Russian ‘critical infrastructure’ is defined in detail in a legal context. In January 2017, a new bill titled “On the Security of Critical Infrastructure of the Russian Federation” was passed that mandates the formation of a special register of all companies and agencies that control objects of critical information infrastructure [15]. It appears that all of the RuNet’s critical infrastructure will fall under complete control of the Russian state authorities and a new official state register of IP addresses for RuNet will appear. Consequently, RuNet has evolved from an alternative social universe to a state-controlled ‘safe and secure’ digital environment manifesting ‘digital sovereignty’.

4 Technical background of 'RuNet 2020'

It has been reported that the Russian authorities (*Minkomsvyaz*, *Roskomnadzor*[3], Ministry of Defence, FSB and Rostelekom) experimented with disconnecting RuNet from the global infrastructure in 2014. Further, it has been stated that during the exercise *Roskomnadzor* ordered communications hubs run by the main Russian Internet providers to block traffic to foreign communications channels by using a traffic control system called Deep Packet Inspection (DPI). However, the experiment failed because thousands of smaller service providers, which *Roskomnadzor* had little control over, continued to pass information out of the country [16]. In addition, Russian officials originally initiated the idea of creating and maintaining a 'back-up-copy' of RuNet in 2014. In this plan the state system would become a 'double' or a 'back-up-copy'[4] of the Internet routing architecture – a database of IP addresses, routing traffic and the DNS system [17] [18] [19].

Starting from June 2016, more detailed technical plans for disconnecting RuNet from the global Internet have been discussed in the press. According to Russian news agencies, an autonomous non-commercial organization MSK-IX, which owns, along with Rostelekom, the largest traffic exchange point in Russia, started to study the formation of 'back-ups' of the RuNet [18] [17] [19]. According to Alexey Platonov, head of MSK-IX, in the first phase they will conduct 'macroscopic studies of the Internet that will be identified as 'walking' traffic and interaction between Autonomous systems. Their study will form the basis for a unified system that will combine the databases of the Dutch RIPE NCC, which is responsible for distributing IP addresses between telecommunications operators, including Russian, and other registries and databases of route information of the internet, i.e. the intention is to make an analogue of RIPE [18]. Currently, each operator independently determines the policy for routing traffic. Companies do not share this information with each other, but 'manifest' their routes in the routing database — the Internet Routing Registry, which is also under the control of the RIPE NCC. Moreover, although the base is rather informational in nature, the operators check the routing tables for constructing their own policies and

[3] *Roskomnadzor* i.e. the Federal Service for Supervision of Communications, Information Technology, and Mass Media was established in 2008. Roskomnadzor is a Russian federal executive body responsible for overseeing the media, including the electronic media, and mass communications, information technology and telecommunications.

[4] The terms for 'back-up' mostly used in Russian are *rezervnaia (kopiia)* (reserve, spare or back-up), *dubl'* (from English word 'double') and more rarely *zerkalo* (a mirror).

destruction of the information in the database may lead to failures throughout the global network [17].

The aim is also to develop a system for visualising traffic in a network to identify problems in routing, and to create a number of web tools that will allow Russian experts to obtain information about network status in real time, and their interaction with each other. The participants in the project argue that a state system similar to the Routing Information Service (RIS), which collects, stores and processes routing information on the Internet, could optimize routing or be more effective in combating DDoS attacks. It is reported that the new system will be non-profit, and its use for domestic operators will be voluntary. In addition, MSK-IX has assured that the project will be completely independent from Rostelekom, because the implementation of the project will be handled by a separate structure — the Fund for the development of network technologies 'Indata' [18] [17] [19]. It has also been noted that other countries are studying the 'infrastructure of the Internet', for instance, companies including RIPE NCC (Netherlands), APNIC (Australia) and CAIDA and FCC (US) [19].

Furthermore, *Minkomsviaz* intends to create its own set register of traffic exchange points and to oblige operators to use only registered points. It will be proposed to holders of these points that they build reserve channels of communication funded from the state budget. Only operators, who have licenses for cross-border data communication, will be able to organise international communication channels. Such international communication is not under the control of SORM[5], which must be installed by all Russian operators [18] [17]. All these proposed technical measures aim to control the Internet routing architecture inside Russia and to be prepared for maintaining operational capabilities outside the global Internet.

5 RuNet between the lines of the Information Security Doctrine (2016)

For over several years, RuNet has been implicitly written in the Russian strategic thinking, e.g. *Minkomsvyaz* has given statements claiming that

[5] SORM (System of Operative Search Methods) started when the Soviet KGB tapped telephones. SORM-2 is a technical system that was used to intercept and analyse the contents of telecommunications within Russia and has extended its reach to monitor the Internet. The SORM-2 programme had access to essentially all information that flows through or originates on the Russian Internet. In addition, SORM-3 encompasses all telecommunications [25, p. 3] [23, pp. 66, 70].

Russia is in need of its own reserve systems [14] [20] [21]. There is a persistent ‘rumour’ in the Russian ‘information space’ that if Russia would occupy, for instance, any European country, all Russian Internet connections would be disconnected in 24 hours [19] [22]. Consequently, there are factual measures that either have been implemented or aim to gradually isolate RuNet from the global Internet infrastructure. Likewise, it is not surprising that the new Information Security Doctrine lists that one of the main aspects of Russian information security is “to deploy a national system for managing the Russian segment of the Internet” [2, p. 29e]. Still, this statement is not elaborated in the document and thus – RuNet needs to be read between the lines.

5.1 Moral purity

According to the doctrine, “increased information influence on the population of Russia, mainly on the young generation, aimed at the erosion of traditional Russian spiritual and moral values” poses a serious threat. Besides, Russia is interested in providing a foreign audience with proper and authentic information about Russian foreign policy and is anxious about the discriminating working environment for Russian journalists abroad [2, p. 12]. Russia has shaped its information space and promoted its natural and self-attained isolation for instance in a project called ‘Clean Internet’ endorsed by *Minkomsvyaz* in 2012. In this project a voluntary association called the ‘Safe Internet League’, that celebrates the ‘closed, safe and secure’ rhetoric, was established [23, p. 298] According to its website, the Safe Internet League is the largest and most reputable Russian organisation fighting dangerous Web content [24]. The ‘Safe Internet League represents’ a model for ‘self-censorship-system’ for a closed network environment and encourages Russian Internet users to stay within the framework of the ‘safe national web’ and this shaping of the information space gives rise to a natural and self-attained isolation.

5.2 Legislative support

Russia has intensively ratified new laws that support the Information Security Doctrine’s objectives. Between 2012 and 2014, the Russian government passed eight laws that aimed at gaining complete control over RuNet [25] [21, p. 175]. These laws allow, for instance, *Roskomnadzor* to block and to censor harmful information and websites deemed extremist or a threat to public order; demand the owners and operators of websites to store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action and to keep this content for six months. The laws also limit anonymous money transfers and donations on the Internet and require all web-based writers (bloggers, social media accounts) with posts that exceed 3,000 page views to register with the government. The laws prohibit the dissemination or re-dissemination (tweeting and retweeting) of 'extremist materials' and require Internet companies, including Google, Twitter, and Facebook, to locate servers handling Russian Internet traffic inside the country and to store their user's data on these locally based servers for a minimum of six months. Furthermore, the legislation prohibits anonymous access to the Internet in public spaces. Moreover, some of these laws have already been tightened during 2015-2016 [21, p. 176] [23, pp. 215-216].

5.3 Domestic solutions

The Information Security Doctrine calls for eliminating the dependence of domestic industries on foreign information technologies and ensuring information security by developing effective Russian technologies [2, pp. 8c, 17]. Over the past years, there have been intentions to develop a 'national operating system' or 'BRICS[6] operating system' that would reduce the dependency on Microsoft Windows [26]. In September 2016, it was reported that the city of Moscow would replace Microsoft programmes with domestic software on thousands of computers [27]. Furthermore, the state media company *Rossiya Segodnya* and Moscow's regional government switched from Oracle database systems to open-source-software (PostgreSQL) maintained by local programmers [27]. In October 2016, it was declared that the Russian 'military Internet' (*voennyi internet*) was fully operational. Officially, the system is called the 'Closed segment for data transmission' and it is not connected to the global Internet and all the computers connected to it rely on domestic components and software [28]. The closed military Internet is a response to the concern that the Russian armed forces' and other state institutions' information security may be threatened by foreign intelligence agencies [2, pp. 11, 16] [9, p. 46g][7]. Moreover, a closed military Internet could serve as a testing ground for domestic hardware and software and manifests independence from the West that is listed as one future aim in the Information Security Doctrine [2, pp. 23d, 23g, 23h]. The need for domestic solutions in the economic sphere is also underlined in the Information Security Doctrine [2, pp. 17, 25b]. In January 2016, it was reported that about a half the Russian banks had turned to using the

[6] BRICS countries – Brazil, Russia, India, China, and South Africa.

[7] The numbers given refer to the Doctrine's section numbers and letters in the Latin alphabet refer to the order not to page numbers.

domestic equivalent to SWIFT [29]. A national payment system would enable independence from the West and could be used together with new allies, for instance, the BRICS countries that aim together to challenge the hegemony of the US in global affairs.

5.4 Strategic partnerships and new governance of information resources

In 2013, the BRICS countries decided to build their own Internet infrastructure 'hidden from the NSA' – to enhance cybersecurity and to create a parallel cyber universe [2, pp. 23c-d]. As the Information Security Doctrine states, the individual states use of technological superiority to dominate the information space threatens the strategic stability of the information space [2, p. 19]. In 2013 it was also announced that they would connect the BRICS counties with a new high-capacity underwater cable that goes from Brazil, around the Cape of Good Hope, northeast up to India, along the Chinese coast and up to Vladivostok in eastern Russia. The length of the fibre-optic cable would be over 33 thousand kilometres, making it one of the most ambitious underwater telecoms projects ever attempted (Figure 2).

The main goal of the project is to create sovereign data access, bypassing all parts of Internet infrastructure located outside the BRICS countries. Russia sees BRICS as an influential global actor with 'its own voice' on cybersecurity issues [30] [31]. In this way Russia seeks to strengthen equal and stable strategic partnerships with 'non-contentious' countries in the field of information security [2, pp. 8e, 28]. Moreover, Russia has declared that the information resources are unequally controlled in the contemporary world order. This inequality threatens the stable and safe functioning of the Internet [2, p. 19].

6 Military tactics and traditional elements of combat power in cyberspace

Throughout human history there has been competition for control of resources and other objectives. In that contest advantage has been achieved by societies and states with more advanced technology and especially the ability to utilise them successfully for military tactics. Traditional elements of combat power constitute firepower, protection, manoeuvre, leadership and information [32, p. 148] via [33, p. 74]. Different states have slightly different elements in their terminologies, but at least manoeuvre, firepower and protection are also found in the set of basic elements in Russian military strategic thinking [33, p. 74]. According to contemporary understanding, successful warfare requires the skilful use and combination of the above combat elements. Alternatively, the basic elements of combat power can be determined also as: ‘influence’, ‘manoeuvre’ and ‘security’ [33, pp. 84-85]. In this article, we apply the more traditional elements since we want to address how the simplicity of ‘old-generation warfare’ is applicable in the abstract and complex cyber domain – where the rules of the physical world and kinetic force are generally considered not to be applicable. We argue that the use of traditional elements of combat power could represent a ‘new-type thinking’ in the cyber warfare context.

In the following, we use the elements in a simplified manner and show their applicability in demonstrating potential military aims. Since cyberspace is a newcomer in the set of military domains, we argue that some ‘cyber elements of combat power’ might be independent. However, we understand that traditionally the combat elements are cross-dependent on each other.

6.1 Manoeuvre

In traditional warfare manoeuvre is often a key element for success. Manoeuvre is utilised for projecting (or concentrating) firepower to achieve advantage over an enemy. It may be understood as the first and most fundamental combat element. By manoeuvring troops skilfully a commander may face the enemy at the most favourable moment and otherwise in the conditions required to defeat the enemy. [32, p. 148] via [33, pp. 74-76]. Manoeuvre can also be an important aspect in providing protection in contemporary warfare.

6.2 Firepower

Firepower can be understood as the ability to project power and have an effect on the enemy’s troops and systems. It consists of the power itself (of the weapons or troops), but on the other hand also that the power may be employed from a distance. To be more specific, troops may have higher firepower than their adversaries if they can project power from a longer distance when compared to the opponent. Traditionally in combats, firepower is applied to destroy or disable the enemy [32, p. 148] via [33, pp. 74-76].

6.3 Protection

Protection is as the ability to defend your own troops from the enemy's firepower in the battlefield. In traditional warfare, protection is achieved via fortification, for example, that prevents the enemy from directly accessing the protected system. On the other hand, fortification may shield the protected system from the firepower of enemy weaponry and enhances the effect of your own weaponry and serves as a platform for observation [34, p. 335]. [32, p. 148] via [33, pp. 74-76]

6.4 Manoeuvre, firepower and protection in cyberspace

The concept of information warfare was already proposed by Arquilla and Ronfeldt in 1992 and the authors analysed cyberwarfare from the combat elements' point of view [35]. Several examples from the history of warfare were given where the better ability to manoeuvre, concentrate and project firepower have been the fundamental reason for victory.

Manoeuvre in cyberspace can be described as "an application of force to capture, disrupt, deny, degrade, destroy or manipulate computing and information resources to achieve a position of advantage in respect to competitors" [36]. It was also discussed how this force in practice would be a code written in order to achieve the attacker's or the defender's objectives by implementing the code at a time and location of their choosing. Consequently, manoeuvre in cyber space is dependent on the concentration (and protection) of firepower, and vice versa, similarly as in traditional warfare. Principles of cyber warfare form a new field in research and the subject seems to be constantly evolving [37]. Furthermore, traditional military principles have been considered and applied in earlier studies [38].

7 Results – the military aim of 'RuNet 2020'

The most evident and desired military aim of 'RuNet 2020' is to enhance protection. This aim is easy to comprehend as protection is "an ability to defend your own troops from an enemy's firepower in the battlefield". The Russians are aiming to enhance their protection by developing domestic hardware and software to reduce dependence on comparable foreign systems. Moreover, by developing an independent and resilient network Russia might be able to convince the outside world that there is no point in attacking its systems [4].

‘RuNet 2020’ would not have any direct effect on Russian firepower. However, if the aim is to achieve higher relative firepower than the expected enemy, one might achieve that by diminishing enemy’s firepower while keeping your own firepower ‘constant’. In practice, entry into potential adversaries’ open networks could be obtained by parallel systems that could be limited for military use only. Furthermore, adversaries’ hardware and software is commonly accessible whereas Russia’s potentially domestic systems would not be. Similarly, the physical presence of the operators in an open society would be moderately easy. We claim that one of the military aims of ‘RuNet 2020’ is that the expected enemy would have lower relative firepower especially when it comes to employing the power *from a distance*.

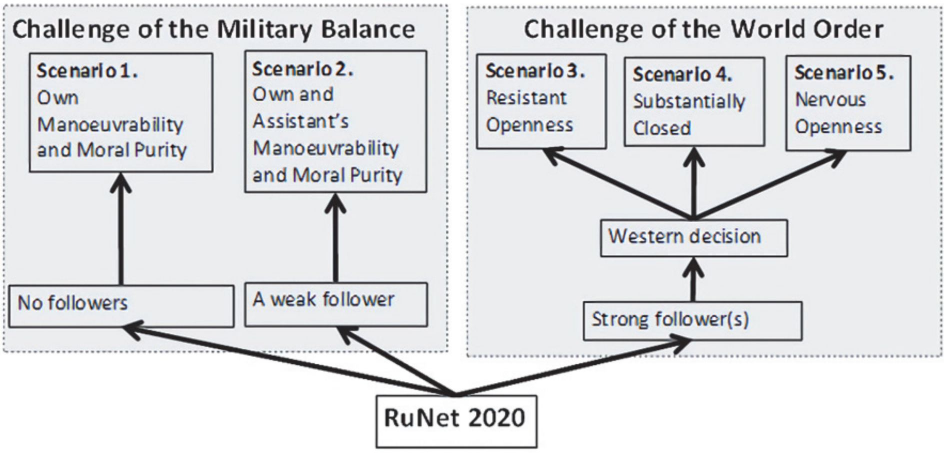
Furthermore, we claim that the Russian military is aiming to achieve better manoeuvrability with ‘RuNet 2020’ and that this is the most significant and unexpected result of this analysis. We do not claim that the manoeuvrability will actually enhanced with ‘RuNet 2020’, but in our understanding the Russian military aim could be based on the following. ‘RuNet 2020’ might be applied in order to gain higher *relative* manoeuvrability than the expected enemy. This is achieved if the enemy’s manoeuvrability is denied by utilising a concealed Internet. Western military operational and tactical networks are concealed as well, but the surrounding societies are dependent on open networks. Therefore, the manoeuvrability of Russian forces at least against those open networks would remain constant. At the same time, the expected enemy’s manoeuvrability within RuNet and against corresponding networks would be lower; at least this is how the expectations of the Russian leadership may look.

The military strategist, and philosopher Sun Tzu once stated that, “Manoeuvring with an army is advantageous; with an undisciplined multitude, most dangerous,” [39, p. 76]. We wonder if this principle has considered when planning RuNet as the analogy between state controlled digital sovereignty (vs. open distributed networks) and an army is quite evident.

8 A game theoretic approach to the potential benefits of ‘RuNet 2020’

We have produced a game theoretical model for envisioning the potential benefits to be gained and the possible paths that could lie behind the Russian strategic thinking if they are able to deploy RuNet and disconnect all its networks from the global Internet (Figure 1). Contrary to traditional

Clausewitzian thinking [40], in this model the West only reacts to Russia's activities, aims and initiatives. This is because Russia's principles go fundamentally against Western ideology, which prevents the West from understanding Russia's mentality in defining cyberspace and cyber warfare [4]. Consequently, the Western lack of awareness results in a reactive mode which is rather close to our simplified model. In our forthcoming research our aim is to further analyse alternative Western choices and their consequences [41].



Challenge of the Military Balance
Scenario 1. Own Manoeuvrability and Moral Purity
Scenario 2. Own and Assistant's Manoeuvrability and Moral Purity
No followers
A weak follower
Challenge of the World Order
Scenario 3. Resistant Openness
Scenario 4. Substantially Closed
Scenario 5. Nervous Openness
Western decision
Strong follower(s)
RuNet 2020

Figure 1. The potential benefits of RuNet for Russia.

The starting point is that Russia deploys RuNet and disconnects all its networks from the Internet [2, p. 29e] [9, pp. 46c-d]. This opening is done in the spirit of Sun Tzu: "…the good fighter is able to secure himself against defeat, but cannot make certain of defeating the enemy" [39, p. 53].

An intermediate step leading to the first scenario is that the path introduced by Russia is not followed by any other states, nor its current or forthcoming allies. This is followed by Scenario 1 called *Own Manoeuvrability and Moral Purity*. In this scenario Russia's own manoeuvrability is higher when compared to all other states. Russia is able to maintain its operational capabilities and ensure its critical information infrastructure in times of peace, under threat of aggression, and during wartime, and to implement separate and independent policies that secure its national interests as planned in the Information Security Doctrine [2, pp. 8b, 29a]. Other benefits are mainly in domestic policy. Russia is able to protect its citizens' 'moral values' by keeping 'harmful information' out [2, pp. 12, 21e]. Nevertheless, this is the least wanted scenario from Russia's perspective.

An intermediate step leading to the second scenario is that only one or a few ‘not-so-powerful states’ (cf. ‘non-contentious’ states [2, pp. 8e, 28]) follow Russia’s example and introduce their own versions of networks disconnected from the global Internet. One of these ‘not-so-powerful states’ could be found for instance among the framework of the Collective Security Treaty Organization (CSTO)[8] or the Commonwealth of Independent States (CIS)[9] [9, p. 21h]. In its Military Doctrine, Russia describes one of the potential areas for military-political cooperation as “the development of dialogue with states concerned about national approaches to counteract the danger of war and military threats posed by the large-scale use of IT-technologies for military and political purposes” [9, p. 55f]. Russia could seek ‘assistants’ by convincing them that it can protect the ‘information space’ of its allies [2, p. 21d].

This is followed by Scenario 2 called *Own and Assistant’s Manoeuvrability and Moral Purity*. In this scenario the benefits for Russia are the same as in the first scenario, but slightly more effective. With the help of even one ‘assistant’ Russia might be able to ‘export’ the ‘close, safe and secure’ narrative and the anti-Western atmosphere to its new potential allies. The narrative could be enforced, for instance, by cognitive-psychological operations reporting how Western ‘openness’ has led to failures in the fight against terrorism [2, p. 29b]. At the same time, Russia could promote ‘RuNet 2020’ as a model for a closed national infrastructure. The Western ‘moral impurity’ exhibited on the global Internet could serve as a ‘common narrative’ for all the potential countries already questioning the contemporary world order [2, p. 23a]. A common denominator for Scenarios 1 and 2 is that the expected benefits are mainly in the military field so we call these scenarios a *Challenge of the Military Balance*.

An intermediate step leading to Scenarios 3, 4 and 5 is at least one ‘powerful state’ or several ‘not-so-powerful-states’ following Russia’s example and introducing their own versions of networks disconnected from the global Internet. One of these ‘powerful states’ could be found for instance among the BRICS countries [9, p. 21g] [2, p. 21d]. This would already have significant information value. Another intermediate step to Scenarios 3, 4 and 5 is that open democratic countries would have to make a decision as to whether they can remain open on this matter or

[8] Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan

[9] Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Uzbekistan

introduce their own 'countermeasures' to reduce their adversaries' manoeuvrability. In Figure 2 we have illustrated how BRICS, CSTO and CIS countries occupy quite large surface area of the globe. It is possible that some other states willing to challenge Western openness would later join the parallel 'cyber universe' or establish their own version of it.

These intermediate steps are followed by Scenario 3 which is called *Resistant Openness* where open democracies choose openness and remain confident with the matter and/or manage to develop countermeasures by using the drawbacks of the closed networks. Russia would still benefit because its own and its allies' manoeuvrability would be higher compared to the open democracies [9, p. 21s]. Moreover, Russia would gain an information victory in that a substantial part of the world would follow its example and it might be able to create suitable international legal mechanisms to prevent and resolve information conflicts [2, p. 29c]. Cognitive-psychological operations would enforce the narrative that the open democracies have failed. Russia together with its allies would aim to rewrite the international legal norms controlling information security to reduce threats to international peace, global and regional security [2, p. 15].

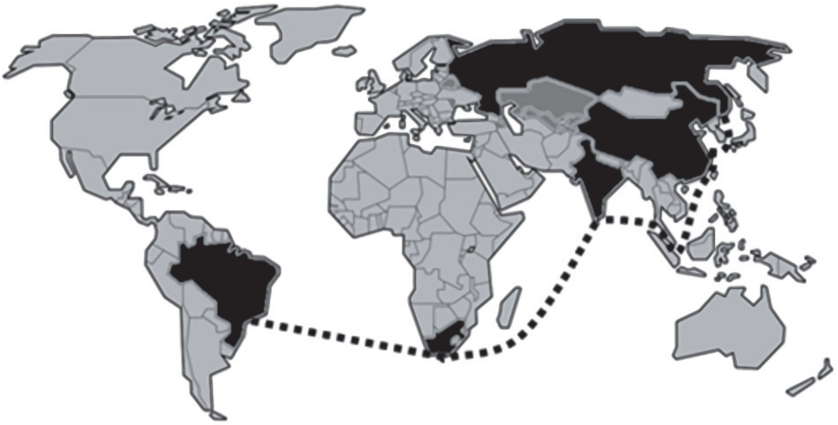


Figure 2. BRICS-countries are shown black and the combination of CSTO and CIS -countries are shown in grey. The schematic outline of the BRICS cable is shown by the dotted line.

Scenario 4 is called *Substantially Closed* where open democracies choose to close their networks extensively and individual freedom of information is excessively controlled by governments. Russia would benefit because it could claim a major information victory – the world would transform into a 'post-western world order' [42]. Russia would have shown the 'correct path' to the whole world where even the open democracies have followed its example and it would fulfil many of the tasks listed in the Information Security Doctrine. From the military point of view this scenario is not as beneficial because the relative manoeuvrability is no longer higher for Russia that its adversaries.

Scenario 5 is called *Nervous Openness*. In this scenario open democracies choose openness, but are not confident about their choice either in a technical or political sense. The open democracies appear indecisive. This might be the most desirable scenario for Russia, because it would benefit the most – it could claim ‘intellectual superiority and digital sovereignty’. Firstly, it could use planned ‘strategic deterrence’ [9] [4] as Russia with its allies would have achieved a higher degree of manoeuvrability than the open democracies. Moreover, the new Russian Information Doctrine states that strategic deterrence and preventing military conflict are among the main reasons for ensuring information security [2, p. 21a]. Secondly, Russia could declare an information victory as it could claim that it had shown the ‘correct path’ to a substantial part of world on the issue. Scenario 5 may also be an intermediate step to both Scenarios 3 and 4. A common denominator for Scenarios 3, 4 and 5 is that the expected benefits are mainly received in the social and/or information domain so we call the scenarios the *Challenge of the World Order*.

9 Conclusions

The initiative for this paper was to experiment with the idea that RuNet will be disconnected technically from the global Internet by controlling the Internet routing architecture inside Russia and that Russia would be able to maintain operational capabilities outside the global Internet by 2020. We have specified the conceptual and technical details of RuNet and shown that the strategy behind RuNet can be analysed using conventional military tactics and the deployment of traditional elements of combat power in the abstract cyber military domain. Our objective has been to discover what Russia’s military aim with ‘RuNet 2020’ could be.

As a result, we argue that the military aim of ‘RuNet 2020’ is not the evident protection improvement, but to improve Russia’s own relative manoeuvrability. In our opinion, the Russian leadership is betting that Russian military’s manoeuvrability, firepower and protection in cyberspace will be higher (relatively) than the expected enemy’s. This holds well especially for manoeuvrability, which is generally understood as the most fundamental combat element. Moreover, ‘RuNet 2020’ could increase Russia’s relative firepower.

On December 22, 2016, Russian President Vladimir Putin spoke at an extended Defence Ministry meeting in Moscow and softly reminded the high military officers that the Information Security Doctrine also concerns the armed forces. Moreover, in the same meeting he powerfully stated that "We can say with certainty: We are stronger now than any potential aggressor. Anyone!" [43]. The following night, President-elect Donald Trump tweeted that "The United States must greatly strengthen and expand its nuclear capability until such time as the world comes to its senses regarding nukes — Donald J. Trump (@realDonaldTrump) December 22, 2016". The following day, December 23, in his annual press conference, Vladimir Putin declared, that Russia would not start an arms race even if Donald Trump promised to expand US nuclear forces. He said, "If anyone unleashes an arms race, it won't be us ... We will never spend resources on an arms race that we can't afford," [44].

There is absolutely no point for Russia to restart the arms race in the field of nuclear forces – as Sun Tzu said: "So in war, the way is to avoid what is strong and to strike what is weak" [39, p. 72]. Therefore, Russia should change the playground and create a 'weak point'. As we have shown, digital sovereignty and RuNet have been written implicitly into the Russian strategic thinking for over several years. As Sun Tzu said: "You may advance and be absolutely irresistible, if you make for the enemy's weak points…" [39, p. 87]. Consequently, digital dependency ('lack of sovereignty') might be the 'weak point' that any potential aggressor would have against Russia.

If Russia succeeds with 'RuNet 2020', it may be exported as a model to its present and forthcoming allies. If, for instance, all the BRICS countries had their own cyberspaces and a common operating system they could offer an optional applicable model to challenge the military balance of the world. Other cultural, religious or linguistic motivations for developing comparable closed networks could lead to fragmentation of the global Internet structure. Inequality in the world order has been expressed by many countries in the BRICS countries and developing nations. If even a few of these 'anti-western' ideologies formed alliances, both the hegemony of the United States and the whole Western world could be challenged. We argue that this is the reason the Russian leadership has faith in 'RuNet 2020'.

As always in game theoretic context it is beneficial to know what players value. Our results are useful for cyber situation awareness and security metrics and especially cyber defence simulation and training, when considering Russia’s potential aim of ruling the cyber and/or information space. Nevertheless, in order to utilise digital sovereignty you have to first create and safeguard it.

Acknowledgment

We wish to acknowledge the expertise of Captain Juha Kukkola (National Defence University), whose observant comments enhanced this paper significantly.

References

[1] P. Lalu, “On war and perception of war Russian thinking: Research Bulletin 2016:3,” 25 May 2016. [Online]. Available: http://puolustusvoimat.fi/documents/1951253/2208221/PVTUTKL_160525_DOS_J_tutkimuskatsaus_on_war_and_perception_of_war_in_Russian_thinking.pdf/2d81a143-9e98-4194-92aa-86157e84b291. [Accessed 24 January 2017].

[2] “Doktrina informatsionnoi bezopasnosti Rossiiskoi Fereratsii [Information Security Doctrine of the Russian Fereration],” 5 December 2016. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. [Accessed 27 December 2016].

[3] S. Makarenko and I. Chucklyaev, “Termonologicheskii basis v oblasti informatsionnogo protivoborstva [The terminological basis of the informational conflict area],” *Voprosy kiberbezopasnosti,* no. 1, pp. 13-21, 2014.

[4] M. Ristolainen, “Should 'RuNet 2020' be taken seriously?,” in *ECCWS*, Forthcomig 2017.

[5] TASS, “Klimenko: Rossiia dolzhna byt' gotova k otkliucheniiu ot mirovogo interneta [Klimenko: Russia should be ready for disconnection from global internet],” 29 December 2016. [Online]. Available: tass.ru/obschestvo/3914882. [Accessed 27 January 2017].

[6] J. Margolin, “Russia, China, and the push for digital sovereignty,” 2 December 2016. [Online]. Available: https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/. [Accessed 30 January 2017].

[7] T. Thomas, “Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?,” *The Journal of Slavic Military Studies,* vol. 27, no. 1, pp. 101-130, 2014.

[8] F. Hare, “The Cyber Threat to National Security: Why can't we agree?,” in *CyCon* , Tallinn, Estonia, 2010.

[9] “Voennaia doktrina Rossiiskoi Federatsii [Military doctrine of the Russian Federation],” 5 February 2010. [Online]. Available: http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf. [Accessed 27 December 2016].

[10] M. Gorham, After Newspeak: Language, Culture and Politics in Russia from Gorbachev to Putin, New York: Cornell University Press, 2014.

[11] E. Zinovieva, “Vozmoshnosti Rossii v global’nom informatsionnom obshchestve [Russia in the global information society],” *Vestnik MGIMO universiteta / MGIMO Review of International Relations,* vol. 48, no. 3, pp. 17-29, 2016.

[12] E. Gorny, A Creative History of the Russian Internet. Studies in Internet Creativity., Berlin: DVM Verlag Dr. Muller, 2009.

[13] I. Ashmanov, “Doklad: Informatsionnyi suverenitet. Sovremennaia real’nost’, [Presentation: Information sovereignty. Contemporary reality],” 24 April 2013. [Online]. Available: http://rossiyanavsegda.ru/read/948/. [Accessed 17 October 2016].

[14] Minkomsvyaz, “Federal’nyi zakon “O vnesenii izmenenii v Federal’nyi zakon “O sviazi” (Proekt) [Federal Law “On the changes to the Federal Law “On connections”],” 11 October 2016.

[Online]. Available: http://regulation.gov.ru/projects#npa=58851. [Accessed 22 October 2016].

[15] "Zakonoproekt No. 47571-7: "O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii" [Bill No. 47571-7: "On the Security of Critical Infrastructure of the Russian Federation]," 2017. [Online]. Available: http://asozd2.duma.gov.ru/addwork/scans.nsf/ID/EBE024490F4C5851432580810054D3AC/$File/47571-7_06122016_47571-7.PDF?OpenElement . [Accessed 6 March 2017].

[16] R. Oliphant, "Russia 'tried to cut off' World Wide Web," 15 October 2015. [Online]. Available: http://www.telegraph.co.uk/news/worldnews/europe/russia/11934411/Russia-tried-to-cut-off-World-Wide-Web.html. [Accessed 19 October 2016].

[17] A. Sukharevskaia and I. Iuzbekova, "Tri voprosa o suverennom runete [Three questions about sovereign RuNet]," *RBK: Ezhednevnaia delovaia gazeta,* 6 June 2016.

[18] A. Sukharevskaia, "Zapasnoi internet: Kto zaimetsia sozdaniem "reservnoi kopii" [Spare internet: Who will establish the "back-up-copy"]," *RBK: ezhednevnaia delovaia gazeta,* 7 July 2016.

[19] D. Nazarov, "Rezervnaia kopiia: Mozhno li otkliuchit' rossiiskii internet ot global'noi seti? [Back-up-copy: Can the Russian segment of the internet be disconnected from the global system?]," 1 September 2016. [Online]. Available: http://www.furfur.me/furfur/freedom/freedom/218695-chto-takoe-rezervnaya-kopiya-interneta. [Accessed 4 October 2016].

[20] A. Golitsyna and A. Prokolenko, "Chnovniki khotiat podchinit' sebe ves' rossiiskii internet [Officials want to supress under their control the entire Russian internet]," 27 May 2016. [Online]. Available: http://www.vedomosti.ru/technology/articles/2016/05/27/642739-

chinovniki-hotyat-internetom. [Accessed 2 November 2016].

[21] P. Vargas-Leon, “Tracking Internet Shutdown Practices: Democracies and Hybrid Regimes,” in *The Turn to Infrastructure in Internet Governance*, New York, Palgrave Macmillan, 2016, pp. 167-188.

[22] R. Rozhkov, “Pervye litsa: ”Internet ”liazhet” na sutki? Ia etogo voobshche ne ponimaiu” Gendirektor TTSI Aleksei Platonov,” *Kommersant',* 18 March 2016.

[23] A. Soldatov and I. Boroganov, The Red Web: The Struggle between Russia’s Digital Dictators and the New Online Revolutionaries., New York: PublicAffirs, 2015.

[24] “Liga bezopasnogo interneta [Safe Internet League],” [Online]. Available: http://www.ligainternet.ru. [Accessed 16 November 2016].

[25] J. Nocetti, “Russia’s ‘dictatorship-of-the-law” approach to internet policy.,” *Internet Policy Review. Journal on Internet Regulation,* vol. 4, no. 4, pp. 1-19, 2015.

[26] “Polnaia videozapis’ repliki Nikolaia Nikiforofa na ”Gaidarovskom Forume 2016”, [Full video clip of Nikolai Nikiforov’s statement at the Gaidar ”Forum 2016”],” 16 January 2016. [Online]. Available: https://vk.com/video292653561_171817033. [Accessed 22 October 2016].

[27] I. Khrennikov, “Moscow Drops Microsoft on Putin’s Call for Self-Sufficiency,” 27 September 2016. [Online]. Available: https://www.bloomberg.com/news/articles/2016-09-27/moscow-drops-microsoft-outlook-as-putin-urges-self-sufficiency. [Accessed 30 September 2016].

[28] V. Zykov and A. Ramm, “V Rossii poiavilsia voennyi internet [A military internet appeared in Russia],” *Izvestiia,* 19 October 2016.

[29] A. Alekseevskikh, “Rossiiskie banki zashchitilis’ ot otkliuchenii iz Briusselia [Russian banks Russian banks protect themselves against outages from Brussels],” *Izvestiia,* 11 January 2016.

[30] J. Nocetti, “Contest and conquest: Russia and global internet governance,” *International Affairs,* vol. 91, no. 1, pp. 111-130, 2015.

[31] A. Gupta, “Cold War-Style ‘Cyber Arms Race’ between US and Russia: Reality or Rhetoric? 98/16,” Center for Air Power Studies, 2016.

[32] J. F. C. Fuller, The Foundations of the Science of War, London: Hutchinson & Co, 1926.

[33] M. Huttunen, Monimutkainen taktiikka [Complex tactics], Helsinki: Maanpuolustuskorkeakoulu,Taktiikan laitos, 2010.

[34] F. D. Margiotta, Brassey's Encyclopedia of Land Forces and Warfare, Washington, 1996.

[35] R. D. Arquilla John, Cyberwar is coming, RAND, 1992.

[36] S. D. Applegate, “The Principle of Maneuver in Cyber Operations,” in *4th International Conference on Cyber Conflict*, Tallinn, 2012.

[37] R. C. Parks and D. P. Duggan, “Principles of Cyber Warfare,” *IEEE Security & Privacy,* vol. 9, no. 5, pp. 30-35, 2011.

[38] S. Liles, M. Rogers, J. E. Dietz and D. Larson, “Applying Traditional Military Principles to Cyber Warfare,” in *4th International Conference on Cyber Conflict*, Tallinn, 2012.

[39] S. Tzu, The Art of war, A Puppet Press Classic, 1910.

[40] C. von Clausewitz, On War, Oxford University Press, 1835, reprint 2008.

[41] J. Kukkola, M. Ristolainen and J.-P. Nikkarila, “Confrontation with Closed National Networks: Open Network Societies' Choices and Consequences,” in *Progress*, 2017.

[42] S. Lavrov, "Foreign Minister Sergey Lavrov’s address and answers to questions at the 53rd Munich Security Conference, Munich, February 18, 2017," 18 February 2017. [Online]. Available: http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2648249 . [Accessed 2 March 2017].

[43] V. Putin, “Rasshirennoe zasedanie kollii Ministerstva oborony [Extended Defence Ministry meeting],” 22 December 2016. [Online]. Available: http://kremlin.ru/events/president/transcripts/53571. [Accessed 28 December 2016].

[44] V. Putin, “Bol’shaia press-konferentsiia Vladimira Putina [the Great Press Conference of Vladimir Putin],” 23 December 2016. [Online]. Available: http://kremlin.ru/events/president/transcripts/53573. [Accessed 28 December 2016].

Confrontation with a closed network nation: Open network society's choices and consequences

Juha Kukkola
Mari Ristolainen
Juha-Pekka Nikkarila

Abstract

The aim of this paper is to understand how closed national networks can impact the future cyber domain from the military perspective. We argue that Russia is currently manipulating the cyber domain through four identified lines of effort that may result in an advantage in a form of asymmetric frontlines on cyber battlefields. Accordingly, a 'closed network nation' will be able to force 'open network society' into a reactive mode. As a result, we present a scenario analysis for the estimation of an open network society's strategic choices and their consequences in a case of escalation and potential confrontation with a 'closed network nation'. This paper improves situational awareness in the cyber domain and supports global planning of cyber operations and defence.

Keywords: Cyber Security, Cyber Operations and Defence, 'Closed national network', 'Open network society', Cyber domain, Cyber battlefield, Asymmetric frontlines, Russia, RuNet

The first version of this paper was published and presented at the Military Communications (MILCOM 2017) conference, Baltimore, USA, October 23-25, 2017.

1 Introduction

The military aspects of the Internet are gaining in strength and at the same time, some nations are shifting away from the original notion of the Internet being open and free. During summer 2016, just as NATO recognized cyberspace[1] as a military domain, Russia declared that RuNet – the Russian segment of the Internet – would be disconnected from the global Internet by 2020. In the recent Information Security Doctrine signed

[1] In this paper the concept 'cyberspace' is defined as "an electronic medium through which information is created, transmitted, received, stored, processed and deleted" [41]. We use the concepts 'cyberspace' and 'cyber domain' separately (cf. footnote 2).

by Vladimir Putin on December 5, 2016, Russia openly aims "to deploy a national system of managing the Russian segment of the Internet" [1].

The aim of this paper is to understand how the underlying dynamics of closed national networks can impact the cyber domain[2]. In our earlier studies we have analysed the possible military aims of 'closed network nations'[3] and have come to the conclusion that their goal is related to enhancing military capabilities (e.g. the basic elements of combat power) when compared with open networks. In other words, it is likely that the motivation behind a closed network nation is to achieve a higher operational capability than that of an 'open network society'[4] [2].

Russia and China are so far the most powerful nations following the closing process[5] [3]. In this paper we take a deeper look into Russia's choices and actions. Russia has not openly promoted the elevation of cyber elements to the military domain in contrast to the USA or NATO. We argue that by using the concept of 'information' instead of 'cyber' when defining its doctrine [4] and forces [5] and pursuing a closed network, Russia is following its own strategy, which aims to achieve a significant advantage in the cyber domain in the form of creating asymmetric frontlines[6] on cyber battlefields[7]. We identify four lines of effort in

[2] The concept 'cyber domain' is understood here as an operational domain that cross-cuts all strategic domains (land, sea, air and space) and has an effect on all other operational domains and is affected by them [40], [36]. In our lexicon 'cyber domain' belongs to military terminology; whereas 'cyberspace' is a common platform (cf. footnote 1).

[3] The concept of a 'closed network nation' is understood in this paper as a nation that is technically able to maintain closed network, i.e. to operate a nationally governed segment of the Internet that can be technically separated from global Internet. The concept is used without quotation marks hereafter.

[4] An open network (i.e. global Internet) is defined in this paper as a network based on a multi stakeholder process, non-nation based governance, public-private partnerships, open access and global connectivity. The open network represents part of the global commons – a collective asset that secures freedom of expression, media pluralism, equal access to knowledge etc. [43, pp. 221-238]. Open network nations share the values of open networks and their segment of the Internet is built on those principles. The open network society is a collection of the above defined nations. The concepts open network, open network nation and open network society are used without quotation marks hereafter.

[5] The 'closing process' concept refers to the process of establishing standards and developing technology and solutions for the ability to nationally control the reliability, integrity and availability of data transfer, storage and processing. The closing process is related to Internet fragmentation as a phenomenon.

[6] 'Asymmetric frontlines' are formed by limiting access into a closed national network, whereas frontlines are absent (by definition) within an open network. Asymmetric frontlines form an intentional weakness for open network societies [28].

[7] A cyber battlefield is an area of confrontation within the cyber domain where adversaries battle for control in order to achieve tactical and operational objectives.

Russia’s strategy and elaborate their outcomes in the future cyber domain from the military perspective.

Based on the identified lines of effort we create a scenario where a closed network nation has shaped the cyber domain to gain an advantage, and thus controls the cyber domain and is able to force an open network society into a reactive mode. Consequently, our objective is to determine the choices available to the open network society and their consequences in the case of escalation and potential confrontation. The overall aim of this paper is to serve as a compass for courses of action in the present, i.e. to improve situational awareness in the cyber domain and to support global planning of cyber operations and defence.

2 Methods and materials

We use a scenario analysis [6] as an experimental methodology for the estimation of open network society’s strategic choices and their consequences in the case of potential confrontation with a closed network nation. Scenario analysis is a tool that allows us to work on the edges of our disciplinary boundaries and consequently, to combine Strategic studies, Russian studies and IT studies in the study of the cyber domain.

Our scenario is built on the information gained from previous Russian and military studies, the National Security Strategy (2015) [7], the 2017-2020 Strategy for the Development of an Information Society (2017) [8], the Information Security Doctrine (2016) [4], and the Military Doctrine of the Russian Federation (2014) [9], in addition to official press releases from Russian Ministries, as well as newspaper articles which in our opinion, reflect potential events that could shape the future. Nevertheless, our aim is to form a scenario according to universal features of closed and open networks in order to address the challenges of Internet fragmentation in general.

We conduct our analysis in three phases. In the first phase we identify Russia’s strategy, lines of effort and objectives. In the second phase we explore the strategic decision-making paths of open network society. In the third phase we analyse the choices and paths in the context of an escalation framework that represents potential consequences in the created scenario.

3 Lines of effort

By analysing Russia's official strategies, doctrines and policy initiatives we claim that Russia's current military objectives are stability, strength, deterrence, and internal information sovereignty in peace time and external information superiority in the potential initial phase of confrontation and during war [7], [4], [9], [10], [11] and [12]. Accordingly, we have identified four lines of effort (LOE) that Russia is pursuing in accordance with its objectives in the cyber domain: propagating 'digital sovereignty', conceptual control, preparation of the cyber domain, and exploiting open society networks. These LOEs are based on Russia's understanding of strategy, war and political struggle [13, pp. 37-80], [14].

3.1 Propagating 'digital sovereignty'

Russia's well documented drive to introduce so called 'digital sovereignty'[8] as an international norm through UN processes can be seen as a direct challenge to multi-stakeholder based open network society [15], [16]. The main agenda of this drive is to couple cyber security with information security and transferring the governance of the Internet to state controlled organizations (i.e. ITU-T). This would allow Russia and its allies to control information flows inside its national borders and also to control the development of the Internet [17]. Russia's interests behind digital sovereignty are manifold. From the military perspective, it allows Russia to mitigate Western dominance in information technology, and furthermore creates legitimacy for closing its networks and supporting national IT-technology. It also enhances mobilization by insulating the population from foreign influence and theoretically provides better protection for critical information infrastructure. It also allows securitizing everything that can be linked to 'information' as military threats deserving appropriate countermeasures [4]. In the global context, by promoting digital sovereignty Russia is trying to dismantle open network society so that it is easier to conduct bilateral power politics, create alliances with likeminded states in cyberspace and promote its authoritarian and nationalistic values [2].

3.2 Conceptual control

We argue that Russia's objective is to control both its national and the global cyber domain with its own and peculiar concepts that differ from

[8] In the Russian approach, 'digital sovereignty' is envisioned as the right and ability of the national government independently to determine national interests in the digital environment [42], [27]. The concept is used without quotation marks hereafter.

the concepts of nations belonging to open network society. In Russian 'cyberspace' is called 'information space' (*informatsionnaia sfera*)[9] or 'information environment' (*informatsionnoe prostranstvo*) reflecting its extensiveness [4]. Russian information space includes all mass media, not only information and computer technology platforms. Moreover, Russia has activated a concept called the 'information counter struggle' (*informatsionnoe protivoborstvo*) [4] that has been inaccurately translated and interpreted as 'information war' in numerous Western studies of Russian cyber strategies. The fundamental problem is that the 'information counter struggle' has never been limited solely to wartime [18]. Initially, Russian theoretical thinking divides 'information counter struggle' into four stages: 1) 'peaceful coexistence' (*mirnoe sosushchestvovanie*); 2) 'conflict of interests' (*stolknovenie interesov*) or continuous 'natural rivalry' (*estestvennoe sopernichestvo*); 3) 'armed confrontation' (*vooruzhennaia konfrontatsiia*); 4) 'war' (*voina*) [19, pp. 276-277], [20] and [21, pp. 20-21].

Russia's perception of information space and 'counter struggle' is shaped by Cold War experiences and thinking. During the Cold War, the Soviet Union considered information warfare to be a natural part of foreign policy in conjunction with all other available means [22]. Today Russia uses this same toolkit, which is evident in Western analysts' use of concepts such as Full-Spectrum Warfare, Hybrid Warfare, Non-linear Warfare, and Heavy Metal Diplomacy to describe Russia's Foreign policy and/or strategy [14], [23], [24] and [11].

3.3 Preparation of the cyber domain

In the Russian mindset, the Internet is a by-product of the dominant American culture and the free information flow proposes a threat to Russian cultural integrity and independence. The RuNet, i.e. the 'Russian Internet' is a relatively closed online environment that is based on the Russian language. Nevertheless, RuNet refers not only to the Russian language, but also to the 'Russian way' of doing things. Generally, RuNet is a self-contained environment with well-developed and highly popular Russian search engines, social networking sites, and free e-mail services. At the beginning, RuNet developed largely free from state influence [25]. However, for the past few years, the Russian government has been significantly tightening the control of Russian information space [8].

Consequently, in summer 2016 the Russian Ministry of Communications (*Minkomsviaz*) declared that RuNet would be disconnected from the global

[9] In this paper all the original Russian concepts and references are given in transliterated form (Library of Congress Transliteration System) and translated into English by the authors.

Internet by 2020 [26]. This statement was reinforced in the new Information Security Doctrine (Dec 5, 2016) where Russia openly aims "to deploy a national system of managing the Russian segment of the Internet" [4]. Thus, 'RuNet 2020' could be seen as a prototype for the development of digital sovereignty [18].

For some time, we have observed how Russia has been conducting intellectual, legislative and technical measures to create a purely domestic network [8], [18]. Furthermore, it seems that Russia is developing both defensive and offensive cyber capabilities to prepare itself for a confrontation in a hostile environment [4]. The 'official Russia' strongly believes in and endorses the endeavour to disconnect the Russian segment of the Internet from the global Internet. The ambition is to maintain operational capabilities outside of the global Internet. Technically, this could be organized with existing technology by using the Border Gateway Protocol (BGP) with an innovative use of Software Defined Networking (SDN) technology [27], [28].

This approach can be viewed from the strategic point of view as preparing the battlefield in the initial period of war (*nachal'nyi period voiny*)[10]. By preparing the national infrastructure and testing offensive cyber capabilities Russia is laying the groundwork for cyber warfare, where it will have a decisive advantage over its opponents.

3.4 Exploiting open society

We consider exploiting open society core values and networks as one line of effort in Russian thinking. This assumption is made on the basis of Russia's strong emphasis on the 'closed, safe and secure' approach, i.e. we argue that an adaptive adversary seeks to exploit vulnerabilities in the opponents' [29], i.e. open society's networks.

Networks in open society consist of both open and restricted networks. For example, military and company networks are closed and secure to a certain extent, for example, because of strict safety standards. However, the surrounding infrastructure networks are at least partially open. Access to the surrounding area of the corresponding interfaces is achievable both physically and technically. Furthermore, open source intelligence can be conducted that gives valuable information about the critical infrastructure (e.g. nation-wide electricity transmission grids combined with spatial and map data) [30]. Because networks are accessible and information is openly available, exploiting open society networks is straightforward.

[10] The term initial period of war and its variations is commonly used in Russian military texts. It emphasizes the need for preparation and decisive action in the first moments of armed conflict [39].

A significant result of the exploitation is potential asymmetry between closed network nations and open network society.[11] In Figure 1, a closed national network is represented by a solid lined ellipse on the right and is surrounded by open network society (i.e. the Internet). For the sake of clarity, in this picture a nation belonging to the open network society is represented by a dotted cloud, despite the fact that in the reality there are no actual borders. There are designated interface(s) at the border of a closed network, and in the figure; there is one on the leftmost border of the closed network. There are no designated interfaces on the border of a nation belonging to the open network society because they are so interconnected.

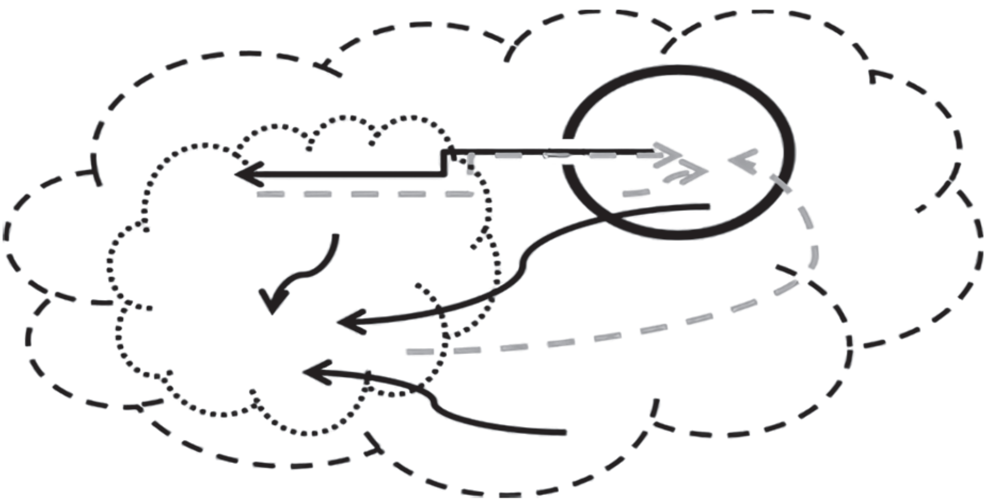


Figure 1: Schematic outline of the open society network's asymmetry with a closed national network.

CNA/CNE[12] operations are marked as arrows in the picture. CNA/CNE operations from the closed national network into the open network nation are shown as a solid line. CNA/CNE operations can be conducted 1) through the designated interface, which is likely to be protected and monitored; 2) through non-designated interfaces; 3) through third party networks; 4) from inside the national network. These operations are rather straightforward to conduct into the open network as we have shown in our earlier studies [2]. CNA/CNE operations into the closed national network are marked as dashed lines that may go 1) through a designated interface; 2) through ad hoc interfaces that require additional measures to penetrate;

[11] We focus on the asymmetry in more detail in our future paper [28], hence in the following we only shortly explain the concept of asymmetry between open and closed networks on the cyber battlefield (Figure 1).

[12] Computer Network Attack / Computer Network Exploitation

3) from inside the closed network. We argue that there is an inherent asymmetry in the frontlines of the future cyber battlefield.

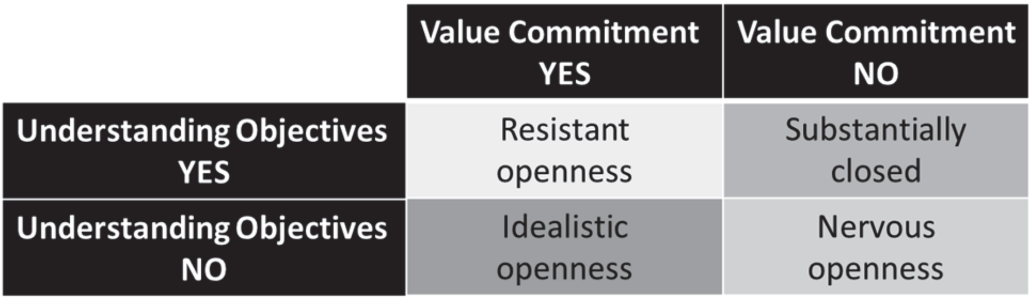
We claim that according to the Russian way of thinking the ‘information counter struggle’ in the cyber domain is a struggle at the strategic level that for the most part is played out during the time of peace. In Russian strategic thinking, these asymmetrical and indirect political, military, societal, economic, informational, and infrastructural actions will neutralize the adversary’s military superiority in general [31], [32]. The lines of effort described in this paper show how Russia is able to play the strengths of a closed national network against the weaknesses of an open network society. Russia is able to shape the cyber domain and achieve at least partial control of it which gives it a degree of freedom of action. This way it has both informational and technological escalation control that can be used to control opponents’ actions thus forcing them into a reactive mode.

4 Scenario: Asymmetric Frontlines

Based on the identified lines of effort we have created a scenario where a closed network nation has shaped the cyber domain into a battlefield with asymmetric frontlines. Accordingly, it has gained an advantage and thus, by exercising control in the cyber domain is able to force open network nations and open network society as a whole into a reactive mode. In the following, we discuss the possible choices open network nations have and their consequences, i.e. paths. Our scenario plays out through a sequence of choices that portray the decision-making process and factors behind it. Finally, the potential consequences are explained through an escalation framework.

4.1 Understanding objectives and value commitment

We have recognised two factors which determine the forthcoming decisions. The first factor is whether open network nations understand the actual objectives of the closed network nation and the threat it poses to open nations (yes/no). We code the factor as ‘yes’ if a nation considers the objectives of closed nations as a threat to national security and basic values. The second factor is whether open network nations identify openness itself as a basic value and are committed to its path(yes/no) (cf. Figure 2).



	Value Commitment YES	Value Commitment NO
Understanding Objectives YES	Resistant openness	Substantially closed
Understanding Objectives NO	Idealistic openness	Nervous openness

Figure 2: Understanding objectives and value commitment

If open network nations do not value their openness and do not understand the objectives of the closed network nations, the most likely outcome is **nervous openness**, i.e. individual countries choose their own way to react separately to the network closing process. In other words, nervousness is a by-product of the distrust of all other nations (including both closed and open nations).

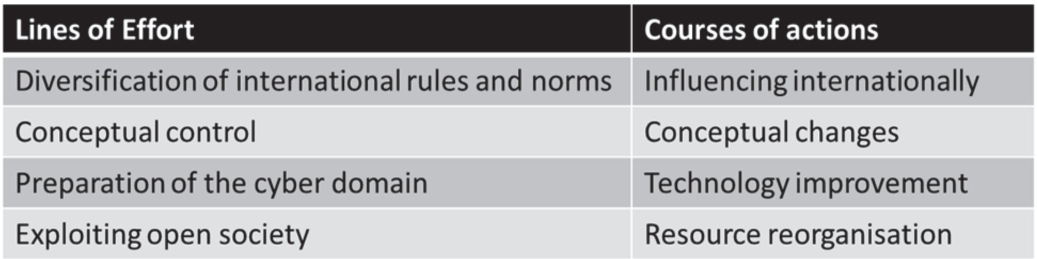
If open network nations do not understand the objectives, but value the openness the most likely outcome of the process is **idealistic openness**. Idealistic openness consists of collective measures, such as defining international norms, diplomacy, economic incentives or pressure. The fundamental principle is a shared disbelief in the technical capability, motivation or the reasonability behind the actions of the closed network nation.

If open network nations understand the objective and do not value openness as a basic principle, the most likely outcome of the chosen process is **substantially closed** networks, i.e. national governments substantially restrict the information flows and connectivity of the network.

If open network nations understand the objectives and value the openness as a basic principle, the potential outcome is **resistant openness**. This is the most prominent path since it is capable of answering to the political and military challenge of closed networks. Thus, in the following we take a deeper look into this path.

4.2 Resistant openness

The path of resistant openness can be divided into four courses of actions: promoting openness, conceptual changes, technology improvement, and resource reorganisation (Figure 3). These courses of actions respond to the lines of effort deployed by closed networks nation explained in section III.



Lines of Effort	Courses of actions
Diversification of international rules and norms	Influencing internationally
Conceptual control	Conceptual changes
Preparation of the cyber domain	Technology improvement
Exploiting open society	Resource reorganisation

Figure 3: Lines of effort vs. Courses of actions

Promoting openness includes the advancement of normative regulation and normative development. Conceptual changes include redefinition of concepts [33], [34] (e.g. ‘counter struggle’) and changing offensive and defensive tactics. Technology improvement constitutes, for instance, dynamically changing IP addresses, research on adversary technology and their technical standard operating procedures (SOPs, e.g. routing). Resource reorganisation makes changes in the legal, technical and economic environment. Resource reorganisation may include aspects such as redefining defence forces’ areas of responsibility and public private partnerships. The mentioned courses of action are somewhat interdependent, e.g. development in the field of technology also induces development of conceptual aspects.

Consequently, resistant openness is achieved by committing intensely to open society’s principles and by disagreeing with the closed nation’s objectives. The strengths of open network nations lie in the capability to reorganize their infrastructure as a society, as well as, to invent and intensively develop new solutions collectively. If the path of resistant openness is chosen, the closed network nation may attempt to change the path to a substantially closed or idealistic open path, e.g. by using information operations. To conclude, we argue that the formation and progress of the most prominent path may face active resistance from the opponent.

4.3 Substantially closed, nervous and idealistic openness

Substantially closed path and path of nervous openness are most likely the main objectives of a closed network nation, especially when analysed in the context of the overall closing process [2]. In the case of substantially closed and nervous openness, part of the objectives of the closed network nation would be achieved. Moreover, in the substantially closed scenario, the closed network nation’s information victory and ‘intellectual superiority' would be evident [2] – the world would be transferred into a desirable "Post-Western World Order" [35].

We have recognized the path of idealistic openness not to correspond to the closed network nation's objectives. Furthermore, idealistic openness can be understood as an intermediate step on the paths both to nervous and resistant openness. The final outcome will depend on how the closed network nation reacts to the chosen course of action of open network nations and society as a whole. The reaction could lead to a redefinition of the closed network nation's objectives, or its continued and active resistance which may force open network nations to choose between resistant or nervous openness.

5 Scenario: Asymmetric Frontlines

The starting point of our asymmetric frontlines scenario was that a closed network nation has forced open network society into a reactive mode. By forcing its adversaries into a reactive mode a closed network nation is able to achieve escalation dominance [36, p. 7]. The level of dominance varies between the different paths. If open societies manage to respond to all the lines of effort and consequently achieve resistant openness and 'information superiority', the escalation could be avoidable. In this case, open network nations could determine the time and instant of the conflict. They would not be critically vulnerable to attacks and could choose from a larger variety of deterrence measures. They would have technical superiority over closed networks and therefore, be able threaten them. Also the actions of the closed network nation could more easily be framed as aggressive according to international rules and norms in the early stages of conflict.

In the substantially closed path, escalation dominance is not achieved by either closed or (currently) open network nations. Therefore, the escalation mechanism in this situation bears similarities to nuclear weapon scenarios where action always requires an immediate counteraction. In this kind of nationalized environment everyone would be vulnerable and ICT infrastructure would be considered a legitimate target of cyber-attack [37]. Because an aggressor would eventually succeed and attribution would be difficult, it could be argued that a first strike would be a prudent policy [38]. Alliances would lose measure of their meaningfulness because there would not be any ICT interdependence to create common interests and an arms race would be inevitable.

The most unfavourable path in the sense of escalation dominance is nervous openness, where the closed network nation determines the location, time and instant of the conflict. Closed network nations could defend themselves from counter attacks, they would decide where the 'red lines' of an armed attack are drawn and they could operate below those lines with freedom. They would have escalation domination: They could strike, but be protected; they could pressure opponents to strike first if that would be politically necessary. A cyber arms race and the non-existence of confidence building measures could lead to unintentional escalation.

It is possible that the path of idealistic openness may only be an intermediate step and its final outcome could be one of the other three paths added with a (possibly) unwanted time delay. The risks related to the idealistic path are high since it relies on the adversary to change its objectives. On the other hand, on the path of idealistic openness, the open network nations may not believe in the (technological) success of the path chosen by the closed nation. Knowledge of the (technological) success or failure of the chosen strategy will be acquired only at the instant of the possible confrontation. Consequently, this makes the path of idealistic openness more risky especially to the open network nations since the closed network nation would have better situational awareness. Closed network societies could renegade and use their advantage while they still have it. Much would depend on regimes, norms and transparency which are all underdeveloped and contrary to the secretive nature of cyber domains.

6 Discussion and Recommendations

The aim of this paper was to understand how the underlying dynamics of closed national networks can impact the cyber domain. We argued that Russia is following its own strategy and constructing its own asymmetric frontlines on the cyber battlefield. In other words, Russia is shaping the cyber battlefield to meet its own objectives. We have identified Russia's four lines of effort and have elaborated their outcomes in the future cyber domain from the military viewpoint.

Each line of effort impacts the ability to shape the battlefield; the freedom of action; the ability to control the opponent; and the potential escalation. These are connected to the ability to threaten the resources and the core values of open network societies. In a confrontation situation this could lead to distrust, an arms race, and at its worst to an unintentional conflict.

Furthermore, each line of effort impacts the available measures in a confrontation situation. In the case of escalation, they determine the strength, starting position and the ability to endure costs of both belligerents. In a worst-case scenario this could lead to a) immediate surrender or b) the usage of extensive force at the beginning of confrontation, which could be one of the military objectives of a closed network nation.

Based on the identified lines of effort we created a scenario where a closed national network has shaped the cyber domain into a battlefield with asymmetric frontlines and is able to force open network society into a reactive mode. We have determined the open network nations’ option space and their consequences in a confrontation situation. Furthermore, we recognized four different paths based on a twofold decision process between understanding the objectives of the closed network nation and commitment to the principal values of an open network society. The recognized paths were: nervous openness, substantially closed, idealistic openness and resistant openness. Resistant openness is the most prominent path since it is capable of answering the political and military challenge of closed networks.

Consequently, our primary recommendation is that in order to avoid the less wanted paths open network nations need to respond as a society to all the lines of effort of closed network nations. Otherwise, open network society will lose control of the cyber domain, and their values and benefits will be degraded, and interests will be weakened in the long run.

A secondary recommendation is that further research should be conducted on network closing processes. Even if our scenarios or interpretations were inaccurate or even erroneous, Internet fragmentation is ongoing. It is most likely that the closing processes are an objective of active military strategic planning due to their obvious impact on operational capabilities.

The third recommendation is to start the necessary planning processes with no further delay. Currently there is no clear strategy formed or developed. Moreover, the subsequent delay favours closed network nations as their planning and implementation processes are already ongoing.

References

[1] “Doktrina informatsionnoi bezopasnosti Rossiiskoi Fereratsii [Information Security Doctrine of the Russian Fereration],” 5 December 2016. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. [Accessed 27 December 2016].

[2] J.-P. Nikkarila and M. Ristolainen, "'RuNet 2020' - Deploying traditional elements of combat power in cyberspace?," in *ICMCIS*, 2017.

[3] N. Inkster, China's Cyber Power, New York: Routledge, 2016.

[4] "Doktrina informatsionnoi bezopasnosti Rossiiskoi Fereratsii [Information Security Doctrine of the Russian Fereration]," 5 December 2016. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. [Accessed 27 December 2016].

[5] S. Shoigu, "Zasedaniia Gosudarstvennoi Dumy [Meeting of the State Duma]," 22 February 2017. [Online]. Available: http://transcript.duma.gov.ru/node/4606. [Accessed 14 March 2017].

[6] H. Kosow and G. Robert, Methods of Future and Scenario Analysis: Overview, Assessment, and Selection Criteria, Bonn: German Development Institute, 2008.

[7] "Strategiia natsional'noi bezopasnosti Rossiiskoi Federatsii [Russian National Security Strategy]," 31 December 2015. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201512310038.pdf. [Accessed 8 March 2017].

[8] "Strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2013 gody [The 2017-2030 Strategy for the Development of an Information Society in the Russian Federation]," 9 May 2017. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf. [Accessed 24 July 2017].

[9] "Voennaia doktrina Rossiiskoi Federatsii [Military Doctrine of the Russian Federation]," 26 December 2014. [Online]. Available: http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf. [Accessed 17 February 2017].

[10] T. Thomas, "Russia 21st Century Information War: Working to Undermine and Destabilize Populations," *Defence Strategic Communications,* vol. 1, no. 1, pp. 11-24, 2015.

[11] M. Galeotti, "Heavy Metal Diplomacy: Russia's Political Use of its Military in Europe Since 2014," ECFR, 2016.

[12] M. Koffman, “The Moscow School of Hard Knocks: Key Pillars of Russian Strategy,” 17 January 2017. [Online]. Available: https://warontherocks.com/2017/01/the-moscow-school-of-hard-knocks-key-pillars-of-russian-strategy/. [Accessed 25 March 2017].

[13] T. Thomas, Russia Military Strategy: Impacting 21st Century Reform and Geopolitics, Fort Leavenworth: Foreign Military Studies Office, 2015.

[14] O. Jonsson and R. Seely, "Russian Full-Spectrum Conflict: An Appraisal after Ukraine," *Journal of Slavic Military Studies,* vol. 28, no. 1, pp. 1-22, 2015.

[15] A. Soldatov and I. Boroganov, The Red Web: The Struggle between Russia’s Digital Dictators and the New Online Revolutionaries., New York: PublicAffirs, 2015.

[16] H. Kwalwasser, "Internet Governance," in *Cyberpower and National Security*, Washington D.C., National Defense University Press, 2009, pp. 491-524.

[17] F. Giacomini and L. Cordani, "Artificial or 'Legitimate' Barriers to Internet Governance?," in *Security in Cyberspace. Targeting Nations, Infrastructures, Individuals.*, New York, Bloomsbury Academic, 2014, pp. 161-182.

[18] M. Ristolainen, "Should 'RuNet 2020' be taken seriously?," in *ECCWS*, 2017.

[19] A. V. Manoilo, Gosudarstvennaia informatsionnaia politika v osobykh usloviiakh [State Information Policy in Special Circumstances], Moskva: MIFI, 2003.

[20] V. Kvachkov, "Spetsnaz Rossii [Russian Special Forces]," Voennaia literatura, 2004. [Online]. Available: http://militera.lib.ru/science/kvachkov_vv/index.html. [Accessed 1 March 2017].

[21] I. Panarin and L. Panarina, Informatsionnaia voina i mir. Informatsionnoe protivoborstvo v sovremennom mire [Information War and Peace. Information Counter Struggle in the Contemporary World], Moskva: OLMA-PRESS, 2003.

[22] K. Pynnönniemi and A. Rácz, "Fog of Falsehood," FIIA Report 45, 2016.

[23] P. A. Karber, "Russian Style Hybrid Warfare," The Potomac Foundation, McLean, VA, January 2015.

[24] B. Perry, "Non-Linear Warfare in Ukraine: The Critical Core Role of Information Operations and Special Operations," *Small Wars Journal,* vol. 11, no. 8, August 2015.

[25] E. Gorny, A Creative History of the Russian Internet. Studies in Internet Creativity., Berlin: DVM Verlag Dr. Muller, 2009.

[26] Minkomsvyaz, "Federal'nyi zakon "O vnesenii izmenenii v Federal'nyi zakon "O sviazi" (Proekt) [Federal Law "On the changes to the Federal Law "On connections"]," 11 October 2016. [Online]. Available: http://regulation.gov.ru/projects#npa=58851. [Accessed 22 October 2016].

[27] A. Streltsov ja P. Pilyugin, "K voprosu o tsifrovom suverenitete [About digital sovereignty]," *Informatizatsiia i sviaz',* nro 2, pp. 25-30, 2016.

[28] J. Kukkola, J.-P. Nikkarila and M. Ristolainen, "Asymmetric frontlines of the cyber battlefields," in *ICCRTS*, In Press 2017.

[29] H. Liddel, The Strategy of Indirect Approach, London: Faber and Faber Limitted London, 1929.

[30] J. Vankka, Ed., Situational Awareness for Critical Infrastructure Protection in Cyber, vol. Report series 1: No 36, Helsinki: National Defence University, 2014.

[31] T. Thomas, "Deciphering Asymmetry's Word Game," *Military Review,* no. July-August, pp. 32-37, 2001.

[32] D. Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," November 2015. [Online]. Available: http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf. [Accessed 2 March 2017].

[33] T. Tuukkanen, "Adapting the Current National Defence Doctrine to Cyber Domain," *International Journal of Cyber Warfare and Terrorism,* vol. 1, no. 4, pp. 32-52, 2011.

[34] J. Anteroinen, Enhancing the Development of Military Capabilities by a Systems Approach, Helsinki: National Defence Univesity, 2013.

[35] S. Lavrov, "Foreign Minister Sergey Lavrov's Address and Answers to Questions at the 53rd Munich Security Conference, Munich, February 18, 2017," 18 February 2017. [Online]. Available: http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2648249. [Accessed 2 March 2017].

[36] M. Libicki, Cyberdeterrence and Cyberwar, Santa Monica: RAND, 2009.

[37] Tallinn Manual 2.0. On the International Law Applicable to Cyber Operations, Cambridge: Cambridge University Press, 2017.

[38] J. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security,* vol. 41, no. 3, pp. 44-71, 2016/17.

[39] T. Thomas, "Thinking Like a Russian Officer: Basic Factors And Contemporary Thinking On The Nature of War," January-March 2016. [Online]. [Accessed 2 March 2017].

[40] NATO, "Comprehensive Operations Planning Directive COPD V2.0," 04 October 2013. [Online]. Available: www.act.nato.int/images/stories/events/2014/sfpdpe/copd_v20.pdf. [Accessed 20 March 2017].

[41] J. B. Godwin III, A. Kulpim, K. F. Rauscher and V. Yaschenko, Eds., Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity. Policy Report 2/2014, EastWest Institute and the Information Security Institute of Moscow State University, 2014.

[42] I. Ashmanov, "Doklad: Informatsionnyi suverenitet. Sovremennaia real’nost’, [Presentation: Information Sovereignty. Contemporary Reality]," 24 April 2013. [Online]. Available: http://rossiyanavsegda.ru/read/948/. [Accessed 17 October 2016].

[43] N. Choucri, Cyberpolitics in International Relations, Cambridge: MIT Press, 2012.

Asymmetric frontlines of cyber battlefields

Juha Kukkola
Juha-Pekka Nikkarila
Mari Ristolainen

Abstract

The fragmentation of the global network progresses towards a formation of national segments of cyberspace walled with 'digital borders'. A number of nations aim to strengthen their sovereignty over the internet by closing their national networks. Russia and China are so far the most powerful nations to implement the closing process. The existing formats for internet governance are becoming outdated, which is followed by an unavoidable threat towards the remaining open-network society – there is no clear line between the concepts of war and peace in cyberspace. In this paper we intend to show how 'digital sovereignty' could be technically structured, what kind of policies it requires and how it would affect future cyber battlefields. 'Digital sovereignty' combined with the ambiguity of conflict creates an asymmetry that can be exploited and used for shaping the cyber domain into a future battlefield with 'asymmetric frontlines'. We claim that the conventional understanding of asymmetry in cyberspace that is based on the problem of attribution will be outdated. Furthermore, our analysis demonstrates how space and time variables form a base for asymmetry in the cyber battlefield of the future. By studying, on the one hand, the creation of asymmetry and on the other its effects on the freedom of action, decision-making and situation awareness of the belligerents, we analyze the creation and dynamics of 'cyber asymmetry'. The overall aim of this paper is to consider what a future cyber battlefield will look like and, at the same time, to improve cyber situation awareness related to the closing process. Finally, we suggest new strategic dilemmas for future study.

Keywords: Battlefield of the future, cyber domain, digital sovereignty, open-network society, closed-network nation, asymmetric frontlines, RuNet

The first version of this paper was published and presented at the International Command and Control Research and Technology Symposium (ICCRTS 2017), Los Angeles, USA, November 6-8, 2017.

1 Introduction

The fragmentation of the global network progresses towards the formation of national segments of cyberspace[1] walled with 'digital borders'[2]. A number of nations aim to strengthen their sovereignty over the Internet by closing their national networks, i.e. the race for 'digital sovereignty'[3] has begun. Russia and China are so far the most powerful nations following the closing process[4] [1], [2]. The existing formats for Internet governance are becoming outdated, which is followed by an unavoidable threat towards the remaining open-network society[5]. Cyberspace is artificial and can be shaped. Thus, it functions as a platform for a new type of asymmetry. Moreover, the current paradigms of conflict have been challenged – there is no clear line between the concepts of war and peace in cyberspace (cf. Russian 'information counter struggle'[6]). These processes together create tension that increases

[1] In this paper the concept of 'cyberspace' is defined as "an electronic medium through which information is created, transmitted, received, stored, processed and deleted" [142, p. 17]. We use separate concepts for 'cyberspace' and 'cyber domain' (cf. footnote 9).

[2] The concept of a border is confusing in the 'borderless' cyberspace. There is no common understanding what borders in cyberspace are or what concept to use (e.g. 'cyber border', 'virtual border', 'unspatialized border', 'iBorder' etc.). In this paper we have decided to use the concept 'digital border', firstly, because it is a direct translation of a concept used in Russian (*tsifrovaia granitsa*) and secondly, the word 'digital' reflects 'computer technology' and 'data processing'. In our understanding, a 'digital border' represents an entity that separates potential national segments of the cyberspace.

[3] In the Russian approach, 'digital sovereignty' is envisioned as the right and ability of the national government to independently determine national interests in the digital environment [20], i.e. cyberspace.

[4] The concept of a 'closing process' refers to the process of establishing standards and developing technology and solutions for the ability to nationally control the confidentiality , integrity and availability of data transfer, storage and processing. The closing process is related to Internet fragmentation as a phenomenon.

[5] An open network (i.e. global Internet) is defined in this paper as a network based on a multi-stakeholder process, non-nation based governance, public-private partnerships, open access and global connectivity. The open network represents part of the global commons – a collective asset that secures freedom of expression, media pluralism, and equal access to knowledge etc. [125, pp. 221-238]. An open-network nation shares the values of open networks and its segment of the Internet is built on those principles. An open network-society is a collection of the above defined nations. The concepts of an open network, an open-network nation and an open-network society are used without quotation marks hereafter.

[6] Russia has activated a concept called 'information counter struggle' (*informatsionnoe protivoborstvo*) [17] that has been inaccurately translated and interpreted as 'information war' in numerous Western studies on Russian cyber strategies. The fundamental problem is that 'information counter struggle' has never been solely limited to wartime (Ristolainen 2017). Initially, Russian theoretical thinking divides 'information counter struggle' into four stages: 1) 'peaceful coexistence' (*mirnoe sosushchestvovanie*); 2)

the probability for nation-state confrontation in cyberspace. The overall aim of this paper is to consider what a future cyber battlefield will look like and, at the same time, to improve cyber situation awareness related to the closing process. Finally, we suggest new strategic dilemmas for future study.

We will continue and deepen the analysis of the potential impact of a closed national network[7] to cyberspace [3], [4], [5].[8] In this paper we are interested in studying how 'digital sovereignty' could be technically structured; what kind of policies it requires; and, how it would affect future cyber battlefields. 'Digital sovereignty' combined with the ambiguity of conflict creates an asymmetry that can be exploited and used for shaping the cyber domain[9] into a future battlefield[10] with 'asymmetric frontlines'[11]. We analyze the formation of imminent 'cyber asymmetry'[12]

'conflict of interests' (*stolknovenie interesov*) or continuous 'natural rivalry' (*estestvennoe sopernichestvo*); 3) 'armed confrontation' (*vooruzhennaia konfrontatsiia*); 4) 'war' (*voina*) [126, pp. 276-277], [124, pp. 20-21].

[7] The concept of a 'closed-network nation' is understood in this paper as a nation that is technically able to maintain a closed network, i.e. to operate a nationally governed segment of the Internet that can be technologically separated from the global Internet. The concept is used without quotation marks hereafter.

[8] In our previous studies, we have discussed the Russian approach to 'digital sovereignty' and the formation of the Russian national segment of the Internet by 2020, i.e. 'RuNet 2020' [3]. Moreover, we have analysed the possible military aims of 'closed-network nations' and have come to the conclusion that their goal is related to enhancing military capabilities (e.g. the basic elements of combat power) when compared with open networks. In other words, it is likely that the motivation of a closed-network nation is to reach a higher operational capability than an 'open-network society' [4]. Furthermore, we have continued to analyse the outcomes of the closing process from the open-network society's point of view and shown how a closed-network nation can shape the cyber domain to gain an advantage and thus, may control the cyber domain and is able to force an open-network society into reactive mode. We have determined an open-network society's choices and their consequences in the case of escalation and potential confrontation [5].

[9] The concept of a 'cyber domain' is understood here as an operational domain that cuts across all strategic domains (land, sea, air and space) and has an effect on all other operational domains and is affected by them [127], [6]. In our lexicon 'cyber domain' belongs to military terminology; whereas 'cyberspace' is a common platform (cf. footnote 1).

[10] In this paper the concept 'battlefield' is understood as a space where military operations are conducted. A 'cyber battlefield' is understood as the digital dimension of a conflict between opposing forces in the cyber domain where military operations are conducted.

[11] Simply, the concept of a 'frontline' is the occupied line that is closest to the enemy. In this paper an 'Asymmetric frontline' is defined as a line of contact that is situated differently for belligerents and gives one of them a clear advantage.

by a closed-network nation. We claim that the conventional understanding of asymmetry (cf. [6]) in cyberspace, which is based on the problem of attribution[13], will be outdated in future battlefields. Our hypothesis is that by creating new frontlines on the cyber battlefields, belligerents can shape battlefield space and time to their advantage. The space and time variables form a base for asymmetry on the future cyber battlefield.

The scope of this paper is limited both temporally and technically. Our focus is on the 'gray zone' [7], [8], and the 'initial period of war'[14] of cyber conflict. That is, the politically ambivalent, militarily restricted and normatively under-regulated continuum that extends from nation state competition all the way to the first open use of armed force. We have restricted our study to using existing protocols: Border Gateway Protocol (BGP) [9] combined with networking architecture Software Defined Networking (SDN) [10] as probable (but not exclusive) technical solutions behind a closed national network, cf. [11]. Although we focus on Russia in this paper, we are open to the notion that our observations could also be applied to other states.

This paper is organized into conceptual and practical parts. In the conceptual part we, firstly, discuss the Russian ambition for 'digital sovereignty'. Secondly, the potential technical solutions for 'digital sovereignty' are explained. Thirdly, the concept of asymmetry is described from different viewpoints. In the practical part we, firstly, present an analytical approach to analyzing cyber asymmetry. Secondly, asymmetry is analyzed through battlefield space and time variables in different types of battlefield scenarios. Thirdly, we present a forecasting model for asymmetric frontlines in the cyber battlefield of the future. And as a conclusion, we will discuss how an open-network society can manage the asymmetry manipulated by a closed-network nation. The main contribution of this paper to the discussions is our analysis of the 'asymmetric frontlines' of future cyber battlefields. The overall aim of this paper is to improve situation awareness in the cyber domain and to suggest new strategic dilemmas for future study.

[12] In this paper 'cyber asymmetry' is based on shaping of cyberspace. 'Cyber asymmetry' affects the freedom of action, decision making and situation awareness of belligerents. The space and time variables play an integral part in 'cyber asymmetry'.

[13] The 'problem of attribution' is understood in this paper as a difficulty to identify a cause or a source of a cyber-attack that can be easily disguised.

[14] The term 'initial period of war' (*nachal'nyi period voiny*) and its variations are commonly used in Russian military texts. It emphasizes the need for preparation and decisive action in the first moments of armed conflict [128].

2 Methods and Materials

Methodologically the conceptual part of this paper is a literature survey of writings pertaining to the Russian view of ‘digital sovereignty’. Also, we use contextual analysis in order to explain the ambiguous ‘asymmetry’ concept used in ‘Western’ and Russian thinking, and military strategies. We do this by separating and explaining several aspects of asymmetry and then recombining them into a fresh and comprehensive understanding of ‘cyber asymmetry’. As a result of the conceptual part, we will generate an analytical approach to comparative analysis of asymmetry in cyber domain.

In the practical part, we will use scenario analysis (cf. [12]) as an experimental methodology for understanding the context of ‘cyber asymmetry’ in different types of battlefields. Finally, we use forecasting modelling (cf. [13], [14]) of a cyber battlefield to define different asymmetric frontlines. Scenario analysis and forecast modelling are methodological approaches that allow us to work on the edges of our disciplinary boundaries and consequently, to combine Strategic studies, Russian studies, and IT technology studies into a study of cyberspace.

Our research material consists of previous Russian, military and cyber studies. One component of our main research material is an article called “About digital sovereignty” (in Russian) by Anatoly Streltsov and Pavel Pilyugin [11]. This work has given us both a conceptual and a technical framework. Additionally, will we use the following materials: the Russian National Security Strategy [15]; 2017-2020 Strategy for the Development of an Information Society in the Russian Federation [16]; and, Russian Information Security Doctrine [17] that in our opinion reflect the potential events that could shape the future cyber battlefields.

3 ‘Digital Sovereignty’ and Post-Western World Order

‘Digital sovereignty’ as a concept has been part of the Russian ‘information space’[15] discussion and research starting from 2012 [18, p. 125], [19, p. 113]. One of the main visionaries behind the concept is an

[15] In Russian ‘cyberspace’ is called ‘information space’ (*informatsionnaia sfera*) or ‘information environment’ (*informatsionnaia prostranstvo*), reflecting its extensiveness. The Russian information space includes all mass media, not only information and computer technology platforms [17].

Internet technologies (IT) expert, Igor Ashmanov [20], who has been envisioning 'digital sovereignty' as a right and an ability of the national government to independently determine geopolitical national interests in the digital environment. In 2016 it was declared that RuNet – the Russian segment of the Internet – would be disconnected from the global Internet by 2020 ('RuNet 2020') and in the Information Security Doctrine, Russia openly aims "to deploy a national system of managing the Russian segment of the Internet" [17]. Nevertheless, there are only a few Russian open source scientific studies on how to establish a closed-network nation and how it connects to achieving 'digital sovereignty' in practice. In their article Anatoly Streltsov[16] and Pavel Pilyugin[17] [11] explain their view on the main components of 'digital sovereignty'; they give the technical parameters of how to maintain a nationally governed network; and, explain how their solutions would erase anonymity, i.e. the problem of attribution in a conflict situation. In the following we summarize Strelsov & Piyugin's [11] designs and present the Russian legal and strategic thinking behind 'digital sovereignty' and explain the political motivation behind the network closing process.

3.1 Border control and governance of 'digital sovereignty'

Streltsov & Pilyugin [11, pp. 25-30] compare 'digital sovereignty' with traditional state sovereignty; they see the Internet as a federation of networks; and, apply simple border theory based on topography in cyberspace. Furthermore, they explain how there are certain rules of how national borders are to be protected and how different subjects (vehicles, goods, people, animals, etc.) can cross national borders. Streltsov and Pilyugin [11, pp. 28-29] suggest that 'digital sovereignty' requires the delineating of cyberspace, i.e. the formation of 'digital state borders'. Similarly, border crossing should be organized through 'digital border crossing points' where the incoming /outgoing (i.e. cross-border) traffic can be monitored. Moreover, they introduce the concept of 'digital customs'. 'Digital customs' would not check all the 'information packets' passing through the 'digital border', but the customs would have a right to monitor the "legitimacy of the information flow" [11, p. 28]. For

[16] Anatoly Streltsov – Deputy Director of the Institute for information security issues of the Moscow State University, doctor of technical sciences, doctor of legal sciences, professor.

[17] Pavel Pilyugin – senior researcher of the Institute of information security issues the Moscow State University, associate professor at Moscow Institute of Electronic technology, candidate of technical sciences.

information security reasons, all of the programs used should be certified by national certification organizations. The national operators (i.e. providers) would be able to organize the traffic, but they would be under the control and supervision of the state. According to Streltsov & Pilyugin [11, p. 29], all of this could be organized with existing technology by using BGP, a standardized exterior gateway protocol designed for exchanging routing and reachability information among autonomous systems (AS) on the Internet. Together with innovative use of e.g. SDN technology, states would be able to form their own policies and reach international or bilateral agreements for the 'digital border' crossing.

Streltsov & Pilyugin [11, p. 29] complain that the contemporary control of Internet traffic based on national providers is technically simpler but it resembles more 'defense lines' than 'digital borders'. Without international agreements the future state cyberspaces will be connected with each other only through nationally controlled gateways, i.e. the Internet as a 'federation of networks' may turn into 'a confederation' (cf. [4]). Moreover, Streltsov & Pilyugin [11, p. 30] conclude their work by resolving the problem of attribution in cyberspace. They suggest that anonymity on the Internet can be erased by different nationally-controlled registration mechanisms of IP-addresses and domains and by state-owned providers of cross-border traffic authentication implementation.

3.2 Legal and strategic governance of 'digital sovereignty'

When reading Streltsov and Pilyugin's [11] article in parallel with the recent Russian legal documents and changes in legislation we find indications that the measures suggested by Streltsov & Pilyugin [11] could be the practical and technical solutions behind the Russian closed national network (cf. 'RuNet 2020'). For example, in 2016, the Russian Ministry of Communications and Mass Media (*Minkomsvyaz*) initiated a law drafting project preliminarily called 'About the Autonomous System of the Internet' [21]. This project consists of two different proposals to update laws called 'On Communications' [22] and 'On Information, Information Technologies and on Information Security' [23] that are closely related to the technical isolation of RuNet. In October 2016, Minkomsvyaz released a draft bill that defines basic Internet infrastructure concepts such as 'autonomous system' and 'infrastructure of the Russian national segment of the Internet' and 'national .ru and .рф zone domain name registrar' from the Russian point of view [22]. The draft bill mandates that the state would control RuNet's entire 'critical infrastructure', including the national .ru and .рф domains, Internet traffic exchange points (IXPs), as well as autonomous systems and networks. Furthermore, updates on the law 'On Information, Information Technologies and on Information Security' were implemented by the Federal Security Service of the Russian Federation (FSB) in December 2016 [23]. The new bill titled 'On the Security of Critical Information Infrastructure of the Russian Federation' was approved at first reading in the state Duma in January 2017 and it will come into force in the beginning of 2018. It mandates that a special register of all companies and agencies that control objects of 'critical information infrastructure' must be formed. Taking all of the legislation for surveillance, control and isolation into account, it seems that a new official state register of IP addresses for RuNet might appear shortly and all of RuNet's 'critical infrastructure' and 'critical information infrastructure' will fall under the complete control of Russian state authors [3].

Overall, information security is part of Russian national security and an object of constant counter-struggle according to the Russian National Security Strategy [15]. Information security includes critical information infrastructure, technological self-sufficiency, political stability and 'spiritual values'. The role of government in securing the 'information sphere' is central [15]. The Doctrine of Information Security [17] states quite clearly that national security is linked to the 'information sphere', i.e. the sum total of technology, information and governance. Threats emanating this 'sphere' can affect even defense, sovereignty and the territorial unity of the Russian state. The military, and especially the intelligence services, have a role in the defense of these, but all in all information security is a centralized, government controlled, whole-of-government, top-down approach. The doctrine clearly sees the 'information sphere' as a space defined by information sovereignty, technological independence and territorial immunity [17].

The Doctrine of Information Security is partially implemented in the Strategy on the Development of Information Society in the Russian Federation for 2017-2030 [16]. The Strategy defines the 'information space' as the technological base of the 'information sphere' and also 'critical information infrastructure' as a collection of information systems, networks, and industrial control systems mainly used by the government and strategic enterprises.[18] The Strategy follows the Doctrine and takes a

[18] The strategy also gives Russian definitions to such modern concepts as IoT, Industrial Internet, Information society, eGovernment, Cloud computing, Big Data, Knowledge society, Digital economy, Fifth generation networks etc.

top-to-bottom approach to building an information society in Russia. The strategy states clearly that ‘the Russian segment of the Internet’ has to be nationally controlled, independent, self-sufficient, protected from outside interference, and under sovereign jurisdictions [16]. Furthermore, the Strategy is executed, for instance, in a State Program ‘Digital Economy of the Russian Federation’, signed in July 28, 2017. It presents a ‘road-map’ tasking that Russia will be digitally sovereign by 2020 and that Russia will be one of the world’s leading countries in the field of information security by 2024 [24].

The idea emanating from these strategies and documents is clear. State sovereignty reaches into cyberspace and has its basis in the modern, territorial state. It is ideologically opposite to ideas about the global commons and the multi-stakeholder model of an open, safe, and secure Internet [3]. These findings seem to be consistent with what Demchak and Dombrowski have called a ‘Cyber Westphalia’ i.e. territorialization of cyberspace [25].

3.3 ‘Digital sovereignty’ as a basis for post-western world order

It seems that Russia would prefer to treat ‘cyber’ as a geopolitical (or ‘geodigital’) territory. Thus, ‘digital sovereignty’ appears to be a logical concept for defining and safeguarding the borders of the Russian ‘information space’ and for ensuring ‘information security’. According to Ashmanov [20], the United States is the only country in the world that has a factual ‘digital sovereignty’. In the Russian approach, the Internet is a by-product of the dominant American culture and therefore, proposes a threat to Russian cultural integrity and independence. The global Internet is dependent on popular applications and services that are provided by the United States based companies that pose a threat to Russian technological integrity and autonomy. Therefore, in the Russian mindset, an asymmetry has developed between Russia, the United States and the North Atlantic Treaty Organization (NATO) that influences the political, ideological, economic and technological fields [26]. Consequently, there exists a long term and serious determination to challenge the US-dominated/led world order [27, p. 19] and progress towards ‘a post-Western world order’ [28].

To summarize, from the Russian point of view the information space clearly belongs to the framework of state sovereignty. This means that there is a tendency to conceptualize it as a state-centric and territorial phenomenon, which is apparent in the effort to build the concept of ‘digital sovereignty.’ The external aspect of this Russian project is to challenge the world order that it perceives as Western and also, by using technical solutions to create a military advantage.

4 Technical Solutions for ‘Digital Sovereignty’

As noted in the previous chapter Streltsov & Pilyugin [11] suggest that ‘digital sovereignty’ could be organized with existing technology by using BGP together with an innovative use of SDN technology[19]. In this chapter we will explain the technical details behind these and consider them as solutions for closing a national network. In the Russian academic field there has been a growing interest in these protocols over the past years, e.g. Krasotin & Alekseev [29]; Konstantinov et at. [30][20]; Chalyy et al. [31][21]; Sosenushkin & Kruglova [32][22]; Chemeritskii [33][23]; and, Patrushev [34][24]. Still, it has to be noted that even if SDN technology brings many benefits to network administration, it has vulnerabilities that weaken its security [35]. The study of these vulnerabilities is not included in this paper.

4.1 Border Gateway Protocol (BGP)

The BGP is a protocol providing connectivity between two or more ASs (networks). It is based on Autonomous System Numbers (ASN) that are

[19] It needs to be noted that theoretically the closing process could be successful by using solely BGP protocol.

[20] Konstantinov et al.’s [30] study considers the issues of using an SDN. The authors have applied several SDN designs in order to enhance a computer cluster performance. They simulated (emulated) a real network and conducted a comparison on different SDN designs. Apparently they emphasize that simulations can be used in order to find out which SDN solution is most suitable for a specified task.

[21] Chalyy et al. [31] bring confidentiality into focus. In other words, how confidentiality may be achieved in an SDN architecture where several agents use the same infrastructure. They propose a specific approach where the controller does not violate the confidentiality and to some extent even integrity.

[22] In their paper, Sosenushkin & Kruglova [32] present an imitation model of a highly utilized network segment under the control of a software defined networking (SDN) controller. A series of modeling experiments is used to prove the efficiency of SDN technology usage for highly loaded network segments.

[23] In his dissertation, Chemeritskii [33] studies and develops methods and tools for evaluating the properties of SDN for known configurations of its components and verifying the compliance properties of these specified routing requirements policies.

[24] Patrushev [34] studies the development of service routing, a method of a global route optimization, QoS parameters that need to be taken into account when calculating the route, end-to-end delay of packet delivery, existing technologies of traffic management service centralized adaptive routing software defined networking.

assigned by the Internet Assigned Numbers Authority (IANA). Basically, the BGP connects individually administered networks to the whole Internet. ISPs can manage one or multiple ASs, and they agree among themselves how these are connected and who routes what traffic. According to its RFC 4271, BGP is to exchange network reachability information with other BGP systems. The correct function of a BGP is based on the mutual trust between the BGP systems. The exchange of reachability information is done manually with updates and withdrawn messages. There is also a possibility to filter these messages [36]. This makes it possible to cut connection at both ends of the BGP links or to change routing information very quickly if necessary [37], [38]. The BGP is an unsecure protocol and it has been targeted by malevolent actors in the past. Attempts to make it more secure with encryption and authentication have stalled because of policy challenges and cost-effectiveness [39].

In the context of Russia's network closing process[25], the connection and disconnection with the rest of the world could be implemented with a BGP. Because there are multiple Local Internet Registries (LIR) (ca. 1400) and ASNs (ca. 5800) in Russia [40], this requires considerable coordination and monitoring in addition to setting up, and administrative and legal procedures. It can be realistically claimed that not all of the information infrastructure of Russian ISPs (etc.) managing those ASNs is located geographically in Russia. Some parts of the networks might even be physically and logically separated from national core networks.

[25] RuNet is built on the physical backbone connections provided mainly by five companies (Rostelkom, MegaFon, MTS, Vimpelkom and TransTeleKom). Optical fiber connects main population centers but microwave and satellite connections are import as well as cellular networks [129]. There are hundreds of ISPs running networks and services although many are local [130]. These are connected in the data link layer by Internet traffic exchange points (IXPs) –the two biggest are MSK-IX (38 nodes with over 500 customer AS) and DataIX (18 nodes with over 150 customer AS) [131], [132]. IXP infrastructure is mostly situated in the western part of Russia or along the Siberian railway route [129]. Routing between ASs is done by BGP4. There are ca. 11 root-level DNS in Russia [133]. MSK-IX is responsible for higher level names server cloud for .ru and .рф domains. It has nodes in 7 federal *okrugs* (i.e. districts) and also abroad. There are governmental and military networks that are more or less separated from private networks (RSNet) [134], [135]. Basically, the majority of the infrastructure is in private hands. The private sector is regulated quite strictly by the Ministry of Telecommunications, Roskomnadzor and FSB [136]. Filtering and black listing are the responsibility of the ISPs, but the government has a SORM-3 system for monitoring and intercepting traffic [137]. Currently RuNet, and the service industry based on it, is growing quite fast and Internet penetration among population is 71.3% [138], [139].

4.2 Domain Name System (DNS) and DNS Security Extensions (DNSSEC)

The BGP is only one element behind the correct operation of the Internet. The Domain name system is a hierarchically distributed registry that provides conversion of host names to IP addresses. In practice, every client must be told where to find its Domain Name Server (DNS) if host names are to be used instead of IP addresses on the Internet. The original description of the DNS function can be found in [41] and [42]. The utilization of DNS is progressing by updates [43], [44], [45].

The DNS security extensions (DNSSEC) add data origin authentication, as well as the data integrity, to the DNS [46], [47], [48]. The root keys of the DNSSEC system are in the possession of the Internet Corporation for Assigned Names and Numbers (ICANN) and stored securely in diverse redundant locations [49].

When it comes to the closing process of the network, the role of the DNS is to conduct address resolution inside RuNet between Russian controlled Top-Level Domains (TLDs) and lower level domains even when the connection to other TLDs is severed. This implies centrally administered national-zone-authority policies to maintain server connections. In this scenario DNSSEC might provide security against third party name-servers masquerading as legitimate name-servers. It is likely that Russia will continue applying DNS with their IP address resolution and construct their whole system accordingly, including the national control of the root keys of the DNSSEC system.

4.3 Software Defined Networking (SDN)

In recent years, there has been a rapidly growing interest in a network technology called Software Defined Networking (SDN) within both the academic community and the industry. An RFC was published on the subject in 2015 [10]. SDN is considered as an emerging paradigm of networking by separating the control logic of a network from the underlying routers and switches; promoting (logical) centralization of network control; and, introducing the ability to program the network [50]. So far, Openflow [51] is the only main protocol supporting the utilization of SDN in practice. With Openflow one may set up a communications protocol between the forwarding layer and different SDN controllers. If Russia pursues a closed network, it is expected that Russia will utilize SDN (via Openflow or a proprietary protocol) in order to execute its routing and control domestically. These solutions would provide a centrally controlled and automated administration of RuNet. Its usage to control an entire country's Internet traffic is likely to require more investigation.

4.4 Possible Russian solution for network closing

As we have stated in chapter 3.2 there is political will to create a national, self-sufficient Internet in Russia. Given time, the outer connections of this network can be controlled with the BGP and the interior network traffic can be controlled by SDN. There is a host of political and financial issues to be solved before this happens, but in an authoritarian country with considerable state participation in the economy and manipulation of public threat perceptions it is only a matter of time. In our understanding the parallel usage of the BGP protocol and the innovative application of SDN architecture is considered to be the most cost effective, easiest, and fastest method to close a national network.

A more extreme measure of control could be national and governmental control of IP addresses and cryptography. By nationalizing the Regional Internet Registry (RIR) services (IP address distributors), establishing a system of fixed addresses, controlling routing information (perhaps by developing local transport and network layer protocols); and, by transparent cryptography, the Russian government could control their national information space. Problems with attribution would be significantly reduced because of a better control and transparency of the ingress traffic into a national network (cf. Chapter 8). All traffic would be transparent for the government and only administratively approved subjects might operate in the network. Because of the economic, legal, political, and technical implications this approach would be costly and in the end it might not work as intended [11, p. 27]. Also, besides or as a replacement for SDN and BGP Russia could employ national, proprietary protocols which would provide security through obscurity to a certain point. In this paper, our focus is on the BGP protocol and SDN technology. However, our aim is to continue and deepen the analysis of the technical solutions behind 'digital sovereignty' in our future studies.

5 Cyberspace and Asymmetry

Political ideas and decisions, governance techniques, and technical solutions form the basis for 'digital sovereignty.' When this sovereignty is claimed unilaterally, it can be considered as an attempt to create asymmetric advantage in cyberspace. This might be considered as the practical aspect of the military nature of 'Cyber Westphalia' [25]. Westphalian sovereignty employed by one state or bloc, but not others, could lead to a considerable military advantage.

Simply, the absence of symmetry creates asymmetry. Yet, the concept of asymmetry is ambiguous and mostly used without a proper understanding of its implications. In this chapter, we focus on 'Western' and Russian asymmetric thinking and military strategies and apply them to cyberspace. Firstly, we will discuss the characteristics of cyberspace. Secondly, we will examine asymmetry as a military theoretical concept. Thirdly, we will combine cyberspace with asymmetry and explore the potential causes of asymmetry in cyberspace. And fourthly, we will reflect on the shaping of cyberspace based on the Russian thinking of asymmetry and 'digital sovereignty'.

5.1 Characteristics of cyberspace

The Internet forms the basic structure of cyberspace. Still, there is no widely accepted definition of cyberspace. Some definitions divide it into constituent parts or different levels. Some focus more on information flows or processes from a holistic point of view. Yet, others concentrate more on the administrational, governmental and legal side of this new, artificial and continually changing space [52, pp. 282-298], [53]. At the turn of the millennium, some envisioned cyberspace as a space transcending the so-called Westphalian state system [54]. This was supposed to be a part of the globalization process that would bring about the disappearance of modern nation states. From this point of view, cyberspace can be viewed as a global commons, a region open to all who have the capability to use it [55], [56].

The global commons thinking is a good starting point for understanding cyberspace as a region characterized by a kind of architecture and model of governance that is naturally symmetrical and flattens the differences in power.[26] Cyberspace can be viewed as a network without a center, flat and free of physical geography. Access to it is cheap and easy, so non-state actors can challenge states and states can use non-state actors as proxies. Distance loses its conventional meaning and time is counted in microseconds, so the ability to make decisions and act quickly is more

[26] It should be pointed out that Joseph Nye Jr. [57, pp. 15-16] criticizes the notion of cyberspace as a 'global commons.' He proposes the term 'regime complex' because there are multiple organizations that regulate cyberspace. The Internet cannot be considered as public goods and a part of the space is in sovereign control.

important than the ability to physically project power [57], [58, pp. 90-91], [52, pp. 309-310]. This means that the resources needed to operate in cyberspace are different than in the physical world. Information, skill, and organization are more important than weapons, transport capabilities or massive manpower [59, p. 108].

From a military perspective, because cyberspace is partly a non-physical, manmade, malleable environment, its relation to other domains is special. Cyberspace penetrates through every other domain. Power can be projected from it, through it, and into it (i.e. kinetic strikes against data centers). Cyberspace is also dependent on other dimensions. There are no communications without cables, satellite links, and data centers [52, pp. 288-289]. There is an ongoing debate, whether cyberspace has a strategic meaning or if it is only an enabling environment, providing support for using force in other domains (cf. [60], [61], [62]). From the global commons point of view cyberspace offers a neutral platform from which to project power globally and instantaneously without the need to worry about borders or national sovereignty. This platform is open to nation states and terrorists alike. It does not enhance the absolute power of non-state actors or weak states, but disperses power and opens new avenues for its use [57, p. 9].

There have been attempts to define illegal actions, armed attacks, and warfare in cyberspace, but this process is still ongoing and has many challenges, cf. Tallinn Manual 2.0 [63] and United Nation Convention on Cooperation in Combating Information Crimes presented by Russia [64]. The Internet is based on a multi-stakeholder model which means that the civil society and non-state actors have an interest in keeping cyberspace out of the control of nation states and supra-governmental authorities [65]. There is also the problem of attribution, which means that because of the way protocols work and the Internet is structured, it is difficult to attribute attacks on information systems on any specific party [66], [67]. Non-governance and non-transparency create an area for different kinds of actors to conduct criminal and subversive operations quite freely.

A major part of the physical infrastructure of cyberspace is owned by private companies, which follow commercial logic and try to stay out of international or local power struggles. Many of the basic services needed for the operation of the Internet are provided by Non-Governmental Organizations (NGOs). Software is produced by international companies [65]. What this means is that it is difficult for an actor or group of actors to try to ‘conquer’ or force their will on any part of cyberspace [6, p. 35]. This digital landscape is constantly changing and resists attempts to control it. Information flows through the path of least resistance. In this context coercive power is based on influencing systems and information, not so much on controlling space or achieving and upholding some kind of superiority over it [68, pp. 37-38], [57, p. 4], [56, p. 44]. At the same time, defense requires constant upgrading, monitoring, and preparations with the view that there is no perfect defense, only resilience [52, pp. 290-291]. *There is no region of cyberspace that is absolutely secure.*

Information societies are dependent on communication and data services. Logistics, finance and critical infrastructure rely on cyberspace. This makes them vulnerable and enticing targets, but state-level attackers are dependent on those same communication and data services, so there is always the possibility of 'mutually assured disruption' [69, pp. 121-122]. Acting in cyberspace requires recognition and access. Traditionally, the attackers have been considered to have the advantage in cyberspace because every system can be breached given time and the defenders are always reacting. Another way to look at this is, that the development and perhaps the normative costs of attacking and one-time use of weapons is so expensive that the use of cyber weapons may not be efficient [70], [71, p. 71]. There is then a logical interest to secure as much of cyberspace under national control as possible. This is of course contrary to the global commons thinking.

If cyberspace gives its own characteristics to the use of power it also affects the threat of use i.e. deterrence. Because there is a problem with attribution, deterring potential attackers is seen to be difficult [57, p. 17]. Also, because cyber capabilities are kept secret, it is difficult to convince potential aggressors about the potential to punish or deter them. Be that as it may, there seems to be progress in the ability to transcend the problem of attribution by combining technical forensics, data on earlier incidents, and political context [71, pp. 51-52]. There have also been cases of shaming and possible multi-spectrum punishment operations against aggressors: for example the United States' operations against North Korea and China [72], [73], [74]. For the time being, the global commons of cyberspace is still a free-for-all environment, including attacks against critical national infrastructure, cf. Prykarpattyaoblenergo, the Democratic National Committee (DNC) hack and WannaCry malware [75], [76], [77].

Based on the description above, we argue that the characteristics of cyberspace seen as a global commons are conducive to symmetry in power. Symmetry rises from the absence of regulative norms, non-transparency, horizontal space, multiple actors, easy access, low costs, and mutual vulnerabilities. In fact, the Internet as a global commons, as an idea and a business model, relies on symmetry. This does not mean that symmetry rules, or that actors strive for it, quite the contrary in fact.

5.2 Asymmetric warfare

Every conflict has asymmetric characteristics [78, p. 22]. There are always vulnerabilities and differences in power. Nevertheless, the concept of 'asymmetric warfare' has appeared and there are universal features how asymmetry is defined in military thinking. Generally, these features relate to unequal military resources and the use of unconventional methods to exploit the vulnerabilities of an adversary.

According to Lawrence Freedman, the idea of asymmetric conflict made its appearance in Western military thinking in the 1970s [79, p. 52]. It was not until the 1990s that asymmetry reached doctrines and strategies, first as an advantage, but quickly changing to vulnerability as the United States began to confront insurgent forces in intervention operations. During the 1990s and 2000s the thinking on asymmetric warfare intertwined with discourses on the revolution on military affairs, network centric warfare and new generation warfare [80], [81], [82], [83], [84]. Behind all this was a discussion on the changing character of war [85], [86], [87]. Basically, asymmetric warfare came to be defined as something done by non-state actors against military superpowers or coalitions that relied on high-tech conventional capabilities and methods, and was restrained by fear of casualties and collateral damage.

There were differences of opinion among what was, basically, a Western community. During the period 1990-2000, there was an argument between the so called Forth Generation Warfare (4GW) thinkers and official network centric warfare proponents. Both tried to legitimize their views on restructuring and re-tasking of modern military forces [88], [89], [90], [91], [92]. The idea, that war was somehow changing with the development of information society, and that networked non-state actors were becoming the principal adversaries, clashed with the idea of the triumph of Western military technology and the continuing relevance of conventional military power that was maintained for intrastate war. There was also conflict between the importance of culture and information versus technology. In the writing of 4GW thinkers, asymmetry was not so much a function of power as a function of will, objectives, organization, and norms regulating behavior.

The evolution of U.S. Joint doctrines introduced ideas about multi-spectrum dominance and cross-domain deterrence [92] which also affected ideas on asymmetry. What these concepts meant from an asymmetrical point of view was that there could be fatal asymmetries in any of the domains of warfare (land, sea, air, space, and cyber) which could be used by an adversary. Already in the 2000s and increasingly in the 2010s military thinkers in the West (and China and Russia) were worried about information as a vulnerability and weapon. It could be used to compel or even to coerce; to win wars without firing a shot by breaking the will of the opponent; to resist or at least paralyze the opponent's military forces. Cyberspace as an infrastructure of information had a prominent role in all of these considerations [93], [79], [6], [94], [2], [95].

The latest incarnation of asymmetry has been the appearance of the so called hybrid warfare. In fact, hybrid warfare has its roots in the same 4GW discussion mentioned above but it was raised to the level of nation states by the illegal annexation of Crimea by the Russian Federation [96], [97], [98]. According to earlier versions of hybrid warfare, asymmetry is not seen so much as a type of conflict or difference in power, but as means and methods. Currently, there is a debate going on if, instead of warfare, we should consider hybrid operations as part of political warfare or as some type of next generation warfare [96], [97], [98], [99]. Because of the international political situation, a more traditional approach to asymmetry has also reappeared: it compares specific capabilities in order to find asymmetry (for example missile defense versus Multiple Independently Targetable Reentry Vehicles (MIRVs)). This is reminisced of the Cold War era calculations. (This is closely related to offense – defense theory [100] and evidence of this thinking can be found in [101], [102] and, on the Russian side, see [99]. Cyberspace has a natural place in this kind of thinking as it provides an avenue for messages, pressuring opponents and the limited use of force under the state of war as a part of normal political competition and, if need be, as a part of escalation.

5.3 Asymmetry in cyberspace

Non-state actors have been on the forefront of security studies concerning cyberspace since 1980s [103, pp. 45-47]. Discourse on cyber terrorism has been ongoing from the 1990s and has had an effect on national cyber security strategies all over the world [95], [104]. Hackers and criminals have also been seen as a serious security threat for the information society. These threats are by their nature asymmetric. Malign state actors made their appearance in official national security discourse as late as in the late 2000s [105]. Not until 2016 was cyberspace designated as a domain of warfare by NATO [106]. Therefore, it is not an exaggeration to state that cyber threats have been traditionally seen as non-state and asymmetric.

Asymmetry in cyberspace can be defined with the same pattern as general asymmetric warfare. Cyberattacks are low-cost and low-risk operations that can be launched from a distance with minimal friendly casualties. They can be used by non-state actors against much more powerful state actors and, theoretically, can inflict massive damage on critical infrastructure, loss of life or at least major political fallout. Cyberattacks use vulnerabilities and provide the ultimate battleground for electronic insurgents because the attacker is free to choose when and where to accept combat and can avoid combat altogether if desired. It is difficult to deter a non-state actor or a state actor using a non-state proxy, and what is more disturbing is that common counterinsurgency methods against attackers do not work ('winning hearts and minds'). The problem of attribution is central to asymmetry. If you do not see or know the attacker, you cannot threaten him or strike back [105], [57, p. 5].

This traditional concept of asymmetry is tied to a notion of weaker, possibly non-attributable non-state actors using unconventional means as the basis for asymmetric warfare. This, we argue, is too limited a perception of asymmetry in cyberspace. The reason is, firstly, cyberspace is artificial and can be shaped according to security needs of states. Secondly, some states are willing to depart from the idea of the global commons towards the concept of nationally controlled closed networks by delimiting networks, controlling infrastructure, and restricting the flow of information. From one point of view, this aspiration to 'digital sovereignty' can be seen as a legitimate effort to limit and contain asymmetry, rising from the dispersion of power and its perceived vulnerabilities. From a different point of view, this process hides behind the building of a different kind of asymmetry.

We argue that this process creates a new kind of asymmetry, which is based on the shaping of the battlefield space and time. By concentrating on traditional asymmetrical threats in cyberspace, and projects to counter them, we miss the deliberate strategy project of Russia, and some other states, to create asymmetry in the battlefield space and time by digitally and physically controlling certain national and territorial parts of the Internet. Their short-term goals are military and economic; the long-term goals are directed against the so-called Western world order.

5.4 Manipulation of asymmetry

Before we move on to a more detailed analysis of asymmetry in cyberspace as a function of the battlefield space and time, we should take note of how Russians understand asymmetry. As we have argued in chapter 4, Russia is one of the states that are striving for 'digital sovereignty.' The Russian understanding of 'asymmetry' implies an active role in changing the symmetry and creating asymmetry (cf. [107, p. 32]). There is a strong connection between non-military and indirect actions, and asymmetrical actions. The idea is to deny the opponent the ability to use force by operating under the level of the open use of force. There should be a continuous search for critical vulnerabilities that might have system-wide effects. By discovering areas where Russia has better combat potential, and thereby using asymmetrical means and methods, a direct military confrontation can be avoided. Information, both its technological and psychological aspect, is seen as a critical aspect of modern warfare. The Russian view is state-centric and based on a perceived technological non-parity with the West (cf. [108, pp. 88, 97, 99, 104]).

Alongside the concept of asymmetry, the concept 'initial period of war' has a central place in Russian military thinking. It concerns the first moments of war which might be decisive in modern high-technology warfare against a technologically superior opponent. This concept underlines the preparation of the battlefield and the ability to fight in the whole depth of the battlefield. This means using all the available means in an integrated fashion from the frontlines to the depth of the adversary's home front, and also defending friendly forces, the society, and state from this kind of attack (cf. [108, pp. 231, 233, 244]). This could be understood as combining the whole government approach to strategic warfare. Asymmetry in conflict t is then achieved by careful preparation already in the 'gray zone.'

The Russian aim is to reverse the asymmetric advantage[27] it perceives the U.S. enjoys in cyberspace. We argue that in order to gain an asymmetric

[27] A Russian concept of 'information asymmetry' exists which is one of the core technologies of the Russian 'information counter struggle' (*informatsionnoe protivoborstvo*) [126, p. 276]. Originally, 'information asymmetry' belongs to economic and contract theory where it is used for creating an imbalance of power in a situation where one party has more or better information than the other. Russian 'information asymmetry' as part of 'information counter struggle' refers to a process where information can be controlled, selected, changed by creating alternative broadcasts, releasing fake news and coverage of events [126, pp. 278-279].

advantage in cyberspace, Russia is preparing to disconnect the Russian segment of the Internet (RuNet) by 2020. The ambition is to control the Internet routing architecture inside Russia and to maintain operational capabilities outside of the global Internet. This would give Russia a decisive advantage when operating in the ‘gray zone’ or during the ‘initial period of war’ (cf. [3], [4], [5]).

Although, there are many similarities in the Russian concept of asymmetry, it differs from the Western one in a few critical aspects. Firstly, it concerns intrastate competition or warfare. Secondly, it sees asymmetry as something that can be created. Thirdly, it is based on the indirect use of force. And fourthly, it has a role before war is declared, but has the greatest impact during the ‘initial period of war’. Based on Russia’s drive towards ‘digital sovereignty’ and the before mentioned differences, we argue that Russia is actively manipulating asymmetry in cyberspace according to its national strategic thinking.

6 Analytical Approach for Studying Cyber Asymmetry

Next, our aim is to broaden the existing traditional strategic, asymmetric, analytical methodologies to cyberspace and to redefine the concept of ‘cyber asymmetry’. We argue that future asymmetry in cyberspace is created by shaping the cyber domain, i.e. that the process of closing national networks creates ‘cyber asymmetry’.

We argue that ‘cyber asymmetry’ should be analyzed through factors that we call ‘asymmetry factors’ in this model. We have deduced these from earlier studies of asymmetry, some of which have been presented in the previous chapter. We are aware that in strategic studies there is a strong critical view on the whole concept of asymmetry. Critics have pointed out that all strategies in all phases of history have tried to achieve asymmetry and find vulnerabilities [109, p. 79], [78, p. 22]. Also, it has been pointed out that asymmetry as an analytical concept has merged with insurgent warfare and nonconventional methods [90], and is a culturally a Western concept [84]. We accept this criticism and try to offer a fresh analytical viewpoint for examining asymmetry in cyberspace.

From previous studies we have deduced at least the following factors concerning asymmetry: Resources (absolute power base), capabilities (relative and contextual power), means (tactics), objectives, will (cost tolerance), norms and culture, organization, information, imagination, space and time [110, pp. 27-30], [111, p. 34], [79, p. 51], [84, p. 125], [90, pp. 636-637], [56, p. 93], [55], [112], [83, p. 2], [80].

The factors we are most interested in are space and time. We are interested in the shaping of cyberspace to achieve asymmetry. Space can be analyzed as distance, borders or environment. In cyberspace, physical distance has little consequences. The digital distance is more important. In this study, we define it as a function of routing (hops, steps, etc.). National or territorial borders have little effect on cyberspace at the moment. Firewalls, filtering, routing, subnetworks and Authentication, Authorization, Audit (AAA) policies have more effect. We are interested in borders because there is a possibility that 'digital sovereignty' will merge territorial and digital borders. The environment is the space where the actors maneuver and act. It consists of geography, roads, weather, and coverage. In the cyberspace environment it depends on the level of analysis. On the physical level it consists of electromagnetic radiation, cables, satellite links, radio connections, routers, and switches. On the syntactic level it consists of networks that are composed of subnetworks, protocols, software, encryption, routes, bandwidth, hosts, services etc. Because cyberspace is partly a non-physical and manmade environment, the norms, rules, and governance are an inherent part of it. They are not scientific laws (i.e. gravity) but changing and open to manipulation. For the above-mentioned reasons, cyberspace is not the same for all or everywhere, and this gives rise to the asymmetrical view of cyberspace.

Time is an important variable because it has a central position in decision-making and in achieving the initiative and attaining surprise. In Western military thinking[28] John Boyd's [113] Observe-Orient-Decide-Act (OODA) –loop has been used to describe a process whereby faster decision-making can give advantage over an opponent, forcing the opponent into a reactive state and perhaps into total collapse. The OODA Loop is a simplified description of decision-making and it can be argued that it does not capture the processes in complex or novel situations very well and gives undue value to the speed of decision-making. Speed, of course is, not everything; lack of time, bad intelligence, or hasty actions can lead to suboptimal decisions.[29] Nevertheless, there is an important temporal aspect in decision-making. An advantage in decision-making speed might give a belligerent the ability to control the escalation by forcing the opponent to react in a certain way by denying it freedom of

[28] For example: JP 3-0 Joint Operations 17 January 2017 [143].

[29] For an alternative and more comprehensive analysis of decision-making, see for example: [140], [141].

action or by threatening important assets. Traditional military thinking also holds that time might be traded for space and vice versa [114, pp. 151-156]. How this happens in cyberspace might be studied by investigating the shaping of cyber battlefields.

We do not argue that a battlefield space and time are the only asymmetry variables affecting cyberspace. But because we are interested in the shaping of cyberspace through 'digital sovereignty' and, specifically, in analyzing how this manipulation affects cyberspace as a battlefield, we see space and time as a good starting point for admittedly complex analysis. Our hypothesis is that by creating new frontlines on cyber battlefields, agents can shape the battlefield space and time to their advantage.

The battlefield space and time are not shaped directly or the engagement frontlines created out of thin air. In the cyber domain, the battlefield space and time are affected by technology, norms, governance, and politics. By studying these it is possible to see where, when, and how asymmetry is deliberately or unintentionally created. Because it is difficult, or perhaps impossible, to directly analyze the battlefield space and time as variables of asymmetry, we concentrate our attention on freedom of action, decision-making, and the situation awareness of agents. We consider variation in these three as the product of battlefield space and time related 'cyber asymmetry'. They all are connected to information which permeates cyberspace as a construct, process, and substance. Because freedom of action, decision-making, and situation awareness are information in a sense, we can measure and analyze them as well.

Because we are interested in the 'gray zone' and the 'initial period of war', 'cyber asymmetry' has two important strategic effects. It relates to attribution and escalation. Advantage in attribution gives an agent the ability to direct its use of force more efficiently and to control the conflict militarily and politically. This means that the problem of attribution is turned from a weakness into strength as a characteristic of cyberspace. The advantage in escalation gives the agent the ability to direct the way the conflict evolves, to react more quickly and to threaten the opponent from a position of strength. We analyze these as strategic concepts as outcomes of 'cyber asymmetry'.

In this study we concentrate on the conceptual-technical level and the governance/political level. The conceptual-technical level concerns standards and their theoretical application and the structure of cyberspace. The governance/political level points our attention to shared norms, sovereignty, use of force, security policies, types of government, organization, and the political context of cyberspace. We impose these limitations on ourselves because we are interested in studying how ‘digital sovereignty’ could be structured (i.e. through BGP and SDN), what kind of policies it requires and how it would affect the future cyber battlefields. We realize that there could be significant technological and practical difficulties in achieving a functioning closed network: it might even lead to catastrophic consequences for the closing nation, but we deem it important to examine the process and consequences nevertheless.

7 Asymmetry in Different Types of Battlefields – Space and Time

Our scenarios start in a situation where Russia declares ‘digital sovereignty’ and disconnects itself from the global Internet. We argue that in this process cyberspace transforms into different types of subspaces. A subspace is inside the cyberspace, but it has a modified topology within itself and in connection with the other subspaces. Thus, technically at least, it relies on the basic structures of cyberspace when transferring information into and out of other subspaces. In this paper, we have identified three potential types of subspace: ‘closed’, ‘open’, and ‘fractured’.

The ‘closed subspace’ is a modified segment of cyberspace where a closed-network nation is technically able to maintain a closed network, i.e. to operate their nationally governed segment of the Internet that can be physically and electronically separated from the global Internet (cf. [5]). In the closed subspace category, we separate the primary-closed subspace, i.e. the segment that is disconnected first (Russia) and the closed subspaces that follow the example of the closing process after the primary-closed subspace.

The ‘open subspace’ is based on the open network. The open network is built upon a society of states. This society is interconnected by a globally accessible network and shares the same basic norms and values concerning information. The open network can be characterized as a global commons. Nevertheless, in this case the ‘open subspace’ functions without one member present, i.e. the closed-network nation that has disconnected its network from the global system and has started to shape the global cyberspace in order to gain an advantage and control that leads to asymmetry.

The ‘fractured subspace’ is a modified segment of cyberspace where several of the nations within the open -network society have decided to substantially restrict the information flows and connectivity of their national network[30] (cf. [1], [2]. In the fractured subspace, individual nations choose their own way to separately react to the network closing processes (cf. secondary-closed subspaces). Some nations might form small alliances, but the general mentality of this subspace is filled with distrust and nervousness. Essentially, a fractured subspace consists of secondary-closed subspaces and the open subspace.

As a result of the process where cyberspace transforms into different types of subspaces, a closed-network nation has managed to shape cyberspace by disconnecting itself from the global Internet. This causes significant structural changes and the division of cyberspace into a mixture of closed and open subspaces that might be followed by further fragmented subspace regiment when the situation develops.

Our scenarios take place in the ‘gray zone’ of conflict during which the above-defined subspaces clash. Moreover, in this phase the cyberspace transform into a ‘cyber domain’. In our lexicon cyberspace is a common platform, whereas ‘cyber domain’ belongs to the military terminology. When the subspaces come into conflict with each other different types of cyber battlefields emerge. In this paper, we have identified three different types of battlefields which feature a closed subspace[31] in the cyber domain: 1) closed vs. open; 2) closed vs. fractured; and 3) closed vs. closed. These battlefields form scenarios where the battlefield space and time asymmetry variables play an integral and prominent part.

7.1 Closed vs. open battlefield

In our previous studies, we have shown how a closed-network nation (e.g. Russia) has the potential to achieve a significant advantage by following its own strategy [5]. Being a nation that disconnects its networks first from the global network, i.e. the primary-closed subspace, it gains a battlefield advantage over those still trusting/upholding open networks.

[30] An example of restricted information flows could serve the Ukrainian block of Russian social media sites (May 2017). This approach promotes an image of a fractured subspace.

[31] Other possible battlefields are: open vs. open, open vs. closed, open vs. fractured, closed vs. closed, closed vs. fractured, and fractured vs. fractured. We recognize that all these battlefields provide interesting scenarios for study. However, we are interest in the ideal type of closed subspace. Therefore, in this paper we do not examine all the possible scenarios.

Russia can control the closed vs. open battlefield with its own concepts that differ significantly from the concepts of nations belonging to an open-network society. Russia's concepts allow it to operate in the 'gray zone' (cf. 'information counter struggle'). Moreover, a closed subspace is centrally controlled and politically solid, i.e. it is able to make fast decisions[32]. However, the open subspace has the potential to self-organize its administrative structure for common situation awareness, i.e. to form a common understanding of the threats because it can openly share information between different agencies (still, in reality the situation awareness is weak). The closed subspace provides technical solutions for monitoring, restricting, and stopping the incoming traffic better than the open subspace. The 'digital border' between these subspaces is clear. Moreover, the technical solutions maximize situation awareness from a closed-network nation's point of view and it can operate more freely in adversaries' networks than adversaries in its networks. Consequently, the engagement space and time asymmetry variables favor a closed-network nation on a battlefield against an open-network society.

7.2 Closed vs. fractured battlefield

When a primary-closed subspace confronts a fractured subspace, the situation is already more complex because there are multiple secondary-closed subspaces. As the fractured subspace consists of secondary-closed subspaces, the freedom of movement is not as significant as in the previous scenario because there is a multitude of borders. Nevertheless, the technical solutions of a primary-closed subspace allow its agents (at least to some extend) to penetrate and operate in the opposition's secondary-subspace networks. Yet, to operate deeply in those networks is challenging because they might have their own borders and proprietary protocols. However, the space asymmetry does not considerably actualize in the closed vs. open scenario because the administrative structure in the fractured subspace is unclear. On one hand, the unclear organizational structure complicates intelligence missions from the primary-closed subspace point of view. Yet, on the other hand, the unclear administrative structure creates difficulties from the defenders point of view. There is no common situation awareness, i.e. no common understanding of the threats because the information material is not shared between information agencies. Moreover, the fractured subspace regime contains different

[32] Authoritarian leader retains as much power and decision-making authority as possible. Authoritarian leaders make decisions independently with little or no input from other people and therefore the decision-making process is relatively faster than for example in a democratic society (cf. [115]).

types of ‘digital borders’ that may cause difficulties to all of the participants of the conflict, i.e. the problem of attribution is at its worst. Furthermore, the time asymmetry advantage is on the side of the primary-closed subspace.

7.3 Closed vs. closed battlefield

In a battlefield where a primary-closed subspace confronts a secondary-closed subspace, the asymmetry of space is minimal because both sides might deploy the same kind of, but technically different, border procedures and protocols. However, the primary-closed subspace always holds an advantage in time asymmetry because it is technically advanced and politically solid for a certain period of time. The so-called ‘asymmetric victory’ is gained via the ‘information victory’ of the primary-closed subspace, i.e. the battle is won without a fight and the world will transform into the so-called ‘post-Western world order’, where there is nothing left of the cyber commons and ‘digital borders’ surround every nation-state.

In this chapter, we have analyzed three different scenarios through conceptual technical and governance/political levels and through the battlefield space and time variables. The scenarios of potential future battlefields indicate how asymmetry is created and how it manifests itself. In the following section, we present a predictive model of asymmetric frontlines in a closed vs. open battlefield.

8 Asymmetric Frontlines and Forecasting Modelling of Cyber Battlefield

In this chapter we focus on the closed vs. open battlefield in more detail as this might be the situation in the near future: because Russia might be actively pursuing this approach and it is also where the ‘cyber asymmetry’ is most apparently explicit. We use forecasting modelling and explain how asymmetric frontlines are formed in this battlefield. The formation of closed vs. open battlefield is demonstrated in Figure 1. The primary-closed subspace is shown encircled on the right, the open subspace is represented as a smaller cloud on the left and the larger cloud containing everything symbolizes the whole cyberspace.

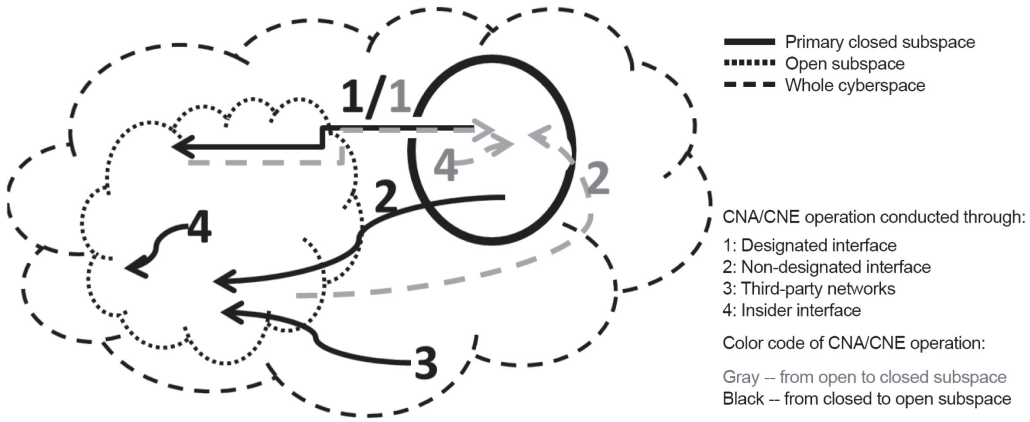

1/1
4
2
4
2
3
Primary closed subspace
Open subspace
Whole cyberspace
CNA/CNE operation conducted through:
1: Designated interface
2: Non-designated interface
3: Third-party networks
4: Insider interface
Color code of CNA/CNE operation:
Gray -- from open to closed subspace
Black -- from closed to open subspace

Figure 1. A schematic view of how Computer Network Attack (CNA)/ Computer Network Exploitation (CNE) operations may be conducted from a closed subspace.

In Figure 1, the arrows illustrate possible Computer Network Attack (CNA)/ Computer Network Exploitation (CNE) operations. The closed subspace is shown encircled, the smaller cloud represents the open subspace and the larger cloud represents the whole cyberspace. Operations from the primary-closed subspace into the open subspace are illustrated as a solid line and operations in the opposite direction are shown as a dashed line. Next, we categorize operations and list and analyze their properties to resolve if asymmetry is present in the new circumstances. The operation categories are: 1) through the designated interface[33]; 2) through non-designated interface; 3) through third party networks; 4) insider interface. In the following sub-chapters we will explain all of the operation categories. First, we examine the effects on the close subspace's defense and second, we study the effects to the closed subspace's offense.

8.1 Designated interface

There are the following effects on the closed subspace's defense: the designated interface is likely to be well-protected and monitored, especially in the direction of the closed subspace. An operation from an open subspace into the closed subspace through this interface is not preferable as the connection may be monitored, controlled, and even blocked when necessary. Even the blocking of all of the traffic can be

[33] A designated interface is, for example, a nationally controlled IPX that has an open interface to ingress / egress traffic to outside networks.

justified as a non-aggressive and defensive action. The possible requirement of an agent or a responsible party for all the traffic into a closed network means that offensive operations will be more difficult. At the minimum, the first indications of harmful traffic are at hand almost immediately when it is detected in a closed subspace. If registration at the 'digital customs' is required (cf. [11, pp. 28-29]) the problem of attribution is diminished. However, the problem of attribution is not entirely solved if the attacker uses third party networks in order to conduct its operation and the registrant is an intermediate victim. Nevertheless, the closed-network nation may trace the attack back to the first step outside its own network e.g. to a liable partner that has agreed to the required conditions. The designated interface provides an undisputable advantage in situation awareness to the closed-subspace defender and, along with centralized monitoring and controlling, enhances decision-making (cf. [115]).

The effects on the closed subspace's offense are the following: An operation conducted from the closed subspace into the open subspace may not currently be controlled as extensively as into the opposite direction. For instance, the origin of the traffic may be hidden almost immediately after crossing the border, for example with IP-hiding services. Even if the monitoring is successful, there are no current methods to prevent such harmful services' actions. The closed-subspace attacker may take advantage of the target nation's information technology infrastructure in its offense and use the designated interface only to deliver the most important commands, thus limiting situation awareness on the open subspace side. If all of the outgoing connections to the open subspace from the closed subspace are disconnected by the open-subspace agent, the closed-subspace actor could see the action as aggressive or even comparable to an armed attack. Nevertheless, the designated interface limits the freedom of action of a closed-subspace attacker. There is at least a theoretical possibility to be caught and more importantly, the operation may be suspended if the open subspace blocks the traffic from the closed subspace. The open-subspace defender has a limited situation awareness and faces the attribution problem. This gives the attacker an advantage in time.

As a result, even if all of the operations go through the designated interface, the differences in situation awareness and the effectiveness of decision show that there is an asymmetry in both the battlefield space and time.

8.2 Non-designated interface

The effects on the closed subspace's defense are the following: The open subspace attacker has to perform additional measures, for example reconnaissance, in order to penetrate into the system. In practice, first the attacker has to find and reconnoiter the interface for the attack. Second, even if the penetration is successful, the legitimacy of the traffic is likely to be checked in every router. Therefore, the attacker has to conduct deceptive actions in order to be able to penetrate into, and to operate within, the closed network. The attack may be disrupted before the actual target and the traffic may be forwarded into the border and/or the incident may be handled as an unauthorized border crossing. The attempt may be considered to be a military action with adequate consequences. Moreover, because the attacker's traffic is unauthorized, it might have problems with protocols, encryption, authentication, and software compatibility. Even if the propagation is successful, there would not necessarily be a control connection available. Therefore, even if a non-designated interface is used, the defender has better situation awareness, decision-making capabilities, and the freedom of action in its own networks.

Effects to the closed subspace's offense are the following: By its definition, the operation is conducted from inside the closed subspace and the primary reason for this would be the straightforwardness of the command line and the execution of the operation. The operation personnel work within the closed subspace's geographical location and the freedom of movement is high. 'Contiguous systems' – yet topologically detached from the closed subspace – may be used for offensive operations through a non-designated interface within the closed subspace. The 'contiguous systems' would likely be separated in both the administrative sense and topologically from the rest of the network. Furthermore, the systems would likely take advantage of the basic structures of cyberspace whenever it is possible. The reason for using the parallel systems could be to hide the origin of the operation. The defender in the open subspace has a full attribution problem, as finding the agent responsible for the assault is both difficult and time consuming. Since this non-designated interface 'does not exist', it creates an additional non-regulated attack vector which may be difficult to analyze and resolve. Because of these restrictions on the open-subspace defender's situation awareness, an attacker may conduct a surprise attack that is difficult to monitor and attribute. A particular challenge is that the execution of the operation requires additional set ups such as the contiguous systems, which might be detected by means outside of cyberspace.

As a result, the use of non-designated interfaces reveals a significant asymmetry between the closed and open subspaces. The asymmetry is mainly expressed through freedom of action and better situation awareness. It is important to note that the majority of the barriers or blockades within the closed subspace do not exist in an open subspace.

8.3 Third party networks

Effects on the closed subspace’s defense are the following: This method is considered implicitly in subchapters 8.1. and 8.2 and consequently is a combination of the methods mentioned therein. When an open subspace attacker uses third party networks for its operation, it is likely to use a non-designated interface. In that case, most of its challenges are mainly related to the penetration and propagation in the defender’s systems. On the other hand, one may use a designated interface, but it is likely that this is addressed in any agreements between the closed subspace and ‘third party networks’ if they exist.

Effects to the closed-network subspace’s offense are the following: Offensive operations conducted via ‘third party networks’ provide even more freedom of action than operations conducted through a non-designated interface. The only drawback is that the operation personnel may have to work in a third party state as well. Yet, one is able to use existing infrastructure in order to conduct the operation. From the defender’s perspective, the problem of attribution may be even higher than in the previous cases. Probably one is able to find out the actual origin (state) of the assault only if the personnel are caught. Otherwise, the signs of the true origin are likely to be masked as ‘cybercriminal’ or ‘hacktivist’ activity. The attacker may conduct its operation from an allied country in order to further complicate the investigation. As in subchapter 8.2., the attacker may conduct a surprise attack and it is almost impossible for the defender to monitor all of the networks of cyberspace. Moreover, closed-subspace operations are possible even if it is disconnected from the global network. The same might not be true with open subspace attackers.

As a result, using ‘third party networks’ provides such as a freedom of action to the closed subspace attacker that asymmetry in the battlefield space and time is considerable.

8.4 Insider interface (requires physical presence in the target country)

Effects to the closed subspace's defense are the following: When building up its defense, a closed subspace is likely to benefit from central control and solid authoritarian politics. Consequently, the attacker may encounter difficulties in infiltrating its personnel into the target region. They may also have to deal with local software and hardware. On the other hand, from the attacker's perspective one may solve the majority of the problems related to penetrating and propagating the defender's systems given enough time for reconnaissance. The defender can frame the issue legally and politically as an aggressive action, even as an act of war. The defender may consider the attackers as conducting a high-risk Special Operations Force (SOF) mission. In the case of an insider threat, the closed-subspace defender's situation awareness is restricted because the system treats the attacker as a legitimate user. The closed-subspace actor's networks are compromised because 'security through obscurity' has been proved faulty. Nevertheless, an authoritarian system enables defender to react quickly and comprehensively if its networks are compromised. And the drawback of the authoritarian system is that it requires societal control, including comprehensive monitoring of its own citizens. During the past years, Russia has intensively ratified new laws[34] for surveillance and control that can be seen as an attempt to solve this challenge (cf. [3]).

Effects to the closed subspace's offense are the following: The information of open-subspace critical systems are either openly available or, at least, can be reconnoitered via the Internet. The information consists

[34] These laws allow, for instance, *Roskomnadzor* (the Federal Service for Supervision of Communications, Information Technology and Mass Media) to block and to censor harmful information and websites deemed extremist or a threat to public order; demand the owners and operators of websites to store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action and to keep this content for six months; limit anonymous money transfers and donations on the internet; require all web-based writers (bloggers, social media accounts) with posts that exceed 3000 page views to register with the government; dissemination or re-dissemination (tweeting and retweeting) of 'extremist materials'; require internet companies, including Google, Twitter, and Facebook, to locate servers handling Russian internet traffic inside the country and to store their users' data on these locally-based servers for a minimum of six months; to prohibit anonymous access to the Internet in public spaces; hold media, news services and search engines liable for all the content in their publications (e.g. linking reposting, and automatically-created links); forbid owners of virtual private network (VPN) services and Internet anonymizers from providing access to websites banned in Russia (cf. [3]).

of physical properties, such as location, the location and types of interfaces, or operation systems' models and versions etc. The corresponding system vulnerabilities are openly downloadable via the Internet. In addition, it is relatively easy to physically reconnoiter interesting locations. It might not even be illegal to some extent. Then again, this method may be the only method where the defender has the authority to verify the incident and is able to sanction the suspects. The defender still has an attribution problem, but it may not be as substantial. Finally, from the attackers' perspective this method is a preferable option only if the previous three methods are not possible.

As a result, in this method the asymmetry is at its lowest level. The battlefield space and time equally affect both belligerents. Still, the differences in the openness of societies that affect the situation awareness give a decisive advantage to the closed-subspace attacker.

8.5 Asymmetric frontlines

As we have shown in subchapters 8.2-8.4, 'cyber asymmetry' manifests most clearly when an open-subspace attacker tries to penetrate into a closed subspace. We will analyze this issue in more detail in the figure below. We argue that the closed subspace can succeed in constructing additional frontlines within its own subspace. The frontlines of a closed subspace are illustrated in Figure 2. The routers are marked with the letter R with a lowering index. For example, BGP refers to the border gateway protocol and SDN to software-defined networking (the routing decisions are conducted at RSDN). The traffic from the border to the target (T) is demonstrated with a dashed line. The ordering of the routers in the mentioned path is represented by router lowering index numbers. The SDN controlled connection between the routers and the SDN control unit (RSDN) is shown as a dotted line. It is important to note that there can be several control units RSDN1, RSDN2 etc., and that they may be located differently than shown in Figure 2.

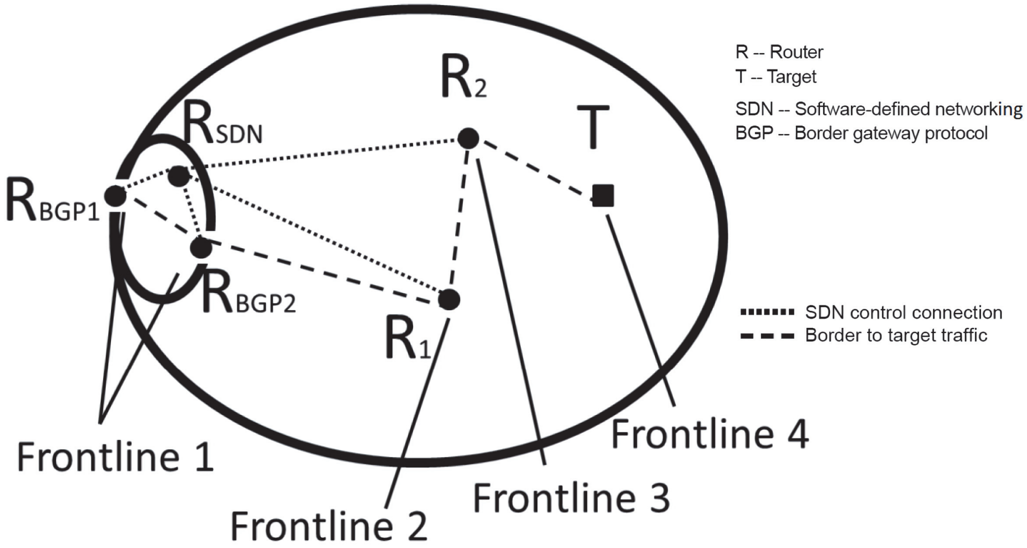


Figure 2. *A simplified schematic outline of the frontlines of a closed subspace. The largest ellipse represents the closed subspace and the smaller demonstrates the 'border crossing-point' and 'digital customs' (cf.* [11]*) between the open subspace and the closed subspace. It needs to be noted that in practice the closed subspace is further divided into several autonomous systems. In the Figure one, the decision-making router RSDN is actually a set of several routers that may be centrally controlled. This kind of administrative structure likely requires the most significant development and resources.*

When an attacker is attacking the target, it faces several challenges on the way before reaching the target itself. The first challenge is at the 'digital border' where the connection author has to register. The source of the connection is verified to be a legitimate source. From the attacker's perspective this is **the first frontline**. Usually, it would not be reasonable to conduct an attack in your own name unless you wanted to perform a show of force. Requiring registration provides additional asymmetry that affects all of the frontlines and it may also have an impact on the political level. The registration can be seen as an attempt to remove or at least to diminish the problem of attribution described in 8.1-8.4. **The second frontline** is at the first router on the path to the target. At the router one can check if the source IP address is a legitimate source, even if the destination IP is permissible, and if the 'digital border crossing' has been authorized, etc. At the second router everything is done again and on top of that one might even check if the route of the connection has been appropriate (**the third frontline**). Consequently, an additional frontline is formed at every router bringing asymmetry into space. The routing tables can be updated straightforwardly and quickly when required, which provides time asymmetry as well. As a result, the attacker has to develop methods to circumvent these frontlines in order to maintain its operational capability.

If the connection to the target is successful, the remaining challenges are related to that IT system's own defensive measures such as firewalls (**the forth frontline**). An additional feature is that the hardware and the software may be different than what used in the open subspace. The difference is mainly a challenge, but on the other hand it may be an opportunity as they will likely have different types of vulnerabilities. The systems of a closed subspace are not threatened by similar types of constant attacks as open networks' operation systems. Therefore, their development may not be as fast and extensive as in the open networks. Finding the vulnerabilities requires syntax understanding and constant learning. As a result, the battlefield space and time asymmetry is formed by the systems' own defensive measures, but the resulting asymmetry does not benefit the closed subspace as drastically as the other frontlines. In other words, an open subspace needs to reconnoiter more and expend more effort in order to maintain its operational capabilities. In addition to the described frontlines, with the help of SDN the traffic can be directed to a honeycomb or a honeypot network on the fly, based on the reliability of the source (cf. [116]).

What makes the frontlines described above asymmetric is that they exist only for one of the belligerents in a potential conflict. An open-network actor's freedom of action, situation awareness, and decision-making are hampered when it conducts offensive operations. On the contrary, the closed-network attacker can operate quite freely in the depth of an open network. Moreover, it confronts frontlines only at the target, if even then. This is the core of the battlefield space and time-based cyber asymmetry.

In our analysis we have shown that the frontlines of a closed network; the possibility to completely disconnect a closed network from other networks; and, the relative freedom of action in open-society networks create a 'cyber asymmetry' that favors a closed-network nation. It has greater situation awareness, a faster decision-making cycle, and more freedom to maneuver than states with an open-network society. It can attack wherever and whenever it wants. It has the advantage in attribution and the ability to control escalation. All this can be achieved already in the 'gray zone', and if a political competition escalates into an open conflict. It will also potentially provide an initiative in cyberspace. This finding corresponds with our earlier studies [5].

9 Results: Cyber Asymmetry and the Battlefield of the Future

The aim of this paper was to consider what a future cyber battlefield could look like. Our paper was divided into conceptual and practical parts that reflect the objective from different perspectives. We have explained how the Russian ambition to 'digital sovereignty' belongs to the framework of state security, and how the external aspect of this project is to challenge the Western world order. Moreover, we argue that the military aim of this Russian project is to gain an advantage and to form an imminent 'cyber asymmetry' that expertly influences future cyber battlefields. The technical solutions in our study were restricted to an existing BGP protocol combined with the SDN networking architecture as a probable technical solution behind the closed national network.

We claimed that the conventional understanding of asymmetry in cyberspace based on the problem of attribution is too limited. We reinforced this argument by explaining the characteristics of cyberspace in relation to asymmetry as a military theoretical concept. Cyberspace is artificial and can be shaped which is at the core of a process where a new kind of 'cyber asymmetry' is created. We argued that by concentrating on traditional asymmetrical threats in cyberspace we miss a deliberate strategy by Russia (and some other states) to manipulate asymmetry digitally and by physically controlling certain national and territorial parts of the open Internet.

We produced an analytical approach for comparative analysis of asymmetry in cyberspace. Our analysis demonstrated how the battlefield space and time variables form a base for asymmetry on the future cyber battlefield. By studying on the one hand the creation of asymmetry and on the other its effects on the freedom of action, decision-making, and situation awareness of belligerents, we could analyze the creation and dynamics of 'cyber asymmetry'. The battlefield space and time variables were observed through changes in these three phenomena.

We presented a scenario where Russia declares 'digital sovereignty' and disconnects itself from the global Internet. We argued that in this process cyberspace could transform into different types of subspaces that are 'closed', 'open', and 'fractured'. The structural changes in cyberspace could increase the probability for a nation state confrontation. When the subspaces collide, different types of cyber battlefields emerge. We analyzed asymmetry through the battlefield space and time variables in different types of battlefield scenarios and showed that belligerents can shape the battlefield space and time to their advantage.

Finally, we focused on the closed vs. open battlefield in more detail as this might be the near future situation and also where ‘cyber asymmetry’ is most explicit. We categorized different CNA/CNE operations and listed their properties and analyzed what effect they have on the closed subspace’s defense and offense. Furthermore, we used forecasting modelling when explaining how a closed subspace can succeed in constructing asymmetric frontlines within its own subspace.

According to our analysis, the future cyber battlefield might be characterized by a new kind of asymmetry, where resources and methods give way to the ability to shape the battlefield space. The frontlines that are different for the belligerents become the source of asymmetry. By creating multiple frontlines in depth based on national control of the Internet, a belligerent can achieve an asymmetric advantage. This advantage can be used in a ‘gray zone’ and the initial period of war to operate more freely; to lessen the problem of attribution (thereby increasing deterrence) and to control escalation by threatening an opponent with disruption and its diminished possibility for a counter strike.

10 Discussion and Recommendations

There is a tendency in Russian foreign policy and security establishments to view Russia as being surrounded by enemies and historically defending itself against outside threats [117], [118], [119]. There is also a school among Western analysts that sees Russia as a defensive great power [120], [121], [122]. At first glance, our findings seem to support these claims. Russia, through ‘digital sovereignty’, is building a strong and resilient cyber defense through a closed subspace. But, as we have shown, in ‘cyber asymmetry’ there is also an inherent advantage to a closed subspace attacker.

In 1725 French engineer Philippe Maigret wrote that: “the best kind of fortresses are those that forbid access to one’s country while at the same time giving an opportunity to attack the enemy in his own territory.” [123, p. 87]. Asymmetric frontlines in cyberspace might not resemble 18th century fortresses but there is a similar logic behind them: Deny and Enable. This digital fortress built on principles of self-sufficiency and deep defense, is constructed during peace time and in a ‘gray zone’ and during the initial phase of a war the asymmetry it creates makes the so called ‘reactive action’ or ‘active defense’ of opponents difficult, or even impossible, to conduct while at the same time enabling offensive cyber operations in the depth of the enemy ‘territory’. If need be, all connections into the cyber/digital fortress can be disconnected and still the digital fortress / agent can support missions outside its ‘walls’.

Even if historical comparisons might be somewhat arbitrary, the ‘cyber asymmetry’ we have described in this paper is real. If Russia chooses to pursue the idea of ‘digital sovereignty’ to its logical end and if it manages to persuade others to follow it, the values and security of the open-network society, based on free, open and secure cyberspace might be in danger. Without a collective approach to this threat, the nations of the open-network society can only close their own national networks. Needless to say, this will make small nations vulnerable, lead to economic problems by destabilizing the global digital economy, erode Western values for the benefit of authoritarian tendencies, and destroy the Internet as we know it.

How then, can the open-network society manage the asymmetry created by closed-network nation(s) without sacrificing its core values? It can start by strengthening the resilience of the open networks and at the same time by studying the vulnerabilities of closed networks to deter those nations from planning to close their networks and thus to keep them open. The open-network society has to prepare for an asymmetric conflict on cyber battlefields if deterrence fails. Taking the easy way and abandoning the open-network society could not provide a military advantage and would truly lead to a post-Western world order. It is tantamount to surrender. The understanding of the cyber battlefields requires a multidisciplinary approach involving all levels of decision-making from the technical to the political and all branches of government. This is not something that individual nations can achieve by themselves. It has to be a collective endeavor.

References

[1] Freedom House, “Freedom on the Net 2016 report,” November 2016. [Online]. Available: https://freedomhouse.org/sites/default/files/FOTN_2016_Full_Report.pdf. [Accessed 24 May 2017].

[2] N. Inkster, China's Cyber Power, New York: Routledge, 2016.

[3] M. Ristolainen, "Should 'RuNet 2020' be taken seriously?," in *ECCWS*, 2017.

[4] J.-P. Nikkarila and M. Ristolainen, "'RuNet 2020' - Deploying traditional elements of combat power in cyberspace?," in *ICMCIS*, 2017.

[5] J. Kukkola, J.-P. Nikkarila and M. Ristolainen, “Confrontation with Closed Network Nation: Open Network Society’s Choices and Consequences,” in *MILCOM 2017*, Baltimore, 2017.

[6] M. Libicki, Cyberdeterrence and Cyberwar, Santa Monica: RAND, 2009.

[7] D. Barno and N. Bensahel, “Fighting and Winning in the "Gray Zone",” 15 May 2015. [Online]. Available: https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/ . [Accessed 15 May 2017].

[8] J. Votel, C. Cleveland, C. Connett and W. Irwin, “Unconventional Warfare in the Gray Zone,” *JFQ,* vol. 80, no. 1st Quarter, pp. 101-109, 2016.

[9] Y. Rekhter, T. Li and S. Hares, “A Border Gateway Protocol 4 (BGP-4)”. Patent RFC 4271, January 2006.

[10] E. Haleplidis, K. Pentikousis, S. Denazis, J. Hadi Salim, D. Meyer and O. Koufopavlou, “Sofware-Defined Networking (SDN): Layers and Architecture Terminology”. Patent RFC 7426, January 2015.

[11] A. Streltsov and P. Pilyugin, “K voprosu o tsifrovom suverenitete [About digital sovereignty],” *Informatizatsiia i sviaz',* no. 2, pp. 25-30, 2016.

[12] H. Kosow and G. Robert, Methods of Future and Scenario Analysis: Overview, Assessment, and Selection Criteria, Bonn:

German Development Institute, 2008.

[13] J. Coates and J. Glenn, "Normative forecasting," in *The millennium project, futures research methodology –V2.0*, J. Coates and J. Glenn, Eds., AC/UNU Millennium Project, 2005.

[14] J. Martino, "A comparison of two composite measures of technology," *Technological Forecasting and Social Change,* vol. 44, pp. 147-159, 1993.

[15] "Strategiia natsional'noi bezopasnosti Rossiiskoi Federatsii [Russian National Security Strategy]," 31 December 2015. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201512310038.pdf. [Accessed 8 March 2017].

[16] "Strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2013 gody [The 2017-2030 Strategy for the Development of an Information Society in the Russian Federation]," 9 May 2017. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf. [Accessed 24 July 2017].

[17] "Doktrina informatsionnoi bezopasnosti Rossiiskoi Fereratsii [Information Security Doctrine of the Russian Fereration]," 5 December 2016. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. [Accessed 27 December 2016].

[18] D. Dubov, "Kibermogushchestvo kak bazis obespecheniia "tsifrovogo" suvereniteta v sovremennom mire: kliuchevie podkhody. [Cyberpower as a fundamental concept for "digital" sovereignty in the contemporary world: Key aspects]," *Oborona i bezopasnost',* vol. 4, no. 25, pp. 123-135, 2014.

[19] J. Nocetti, "Contest and conquest: Russia and global internet governance," *International Affairs,* vol. 91, no. 1, pp. 111-130,

2015.

[20] I. Ashmanov, "Doklad: Informatsionnyi suverenitet. Sovremennaia real'nost', [Presentation: Information Sovereignty. Contemporary Reality]," 24 April 2013. [Online]. Available: http://rossiyanavsegda.ru/read/948/. [Accessed 17 October 2016].

[21] A. Golitsyna and A. Prokolenko, "Chnovniki khotiat podchinit' sebe ves' rossiiskii internet [Officials want to supress under their control the entire Russian internet]," 27 May 2016. [Online]. Available: http://www.vedomosti.ru/technology/articles/2016/05/27/642739-chinovniki-hotyat-internetom. [Accessed 2 November 2016].

[22] Minkomsvyaz, "Federal'nyi zakon "O vnesenii izmenenii v Federal'nyi zakon "O sviazi" (Proekt) [Federal Law "On the changes to the Federal Law "On connections"]," 11 October 2016. [Online]. Available: http://regulation.gov.ru/projects#npa=58851. [Accessed 22 October 2016].

[23] "Zakonoproekt No. 47571-7: "O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii" [Bill No. 47571-7: "On the Security of Critical Infrastructure of the Russian Federation]," 2017. [Online]. Available: http://asozd2.duma.gov.ru/addwork/scans.nsf/ID/EBE024490F4C5851432580810054D3AC/$File/47571-7_06122016_47571-7.PDF?OpenElement . [Accessed 6 March 2017].

[24] "Programma:"Tsifrovaia ekonomika Rossiiskoi Federatsii" [State Project: Digital Economy of Russian Federation]," 28 June 2017. [Online]. Available: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf. [Accessed 3 August 2017].

[25] C. Demchak and P. Dombrowski, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs,* vol. International Engagement on Cyber III,

no. 29-38, 2013.

[26] M. Kucheriavyi, Informatsionnye izmerenie politiki natsional’noi bezopasnosti Rossii v usloviiakh sovremennogo globalnogo mira [Information Dimensions of the Russian National Security Policy in the Modern Global World], St. Petersburg: PhD-Dissertation, Saint Petersburg State University, 2014.

[27] D. Trenin, Should We Fear Russia?, Cambridge: Polity Press, 2016.

[28] S. Lavrov, "Foreign Minister Sergey Lavrov’s Address and Answers to Questions at the 53rd Munich Security Conference, Munich, February 18, 2017," 18 February 2017. [Online]. Available: http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2648249. [Accessed 2 March 2017].

[29] A. Krasotin and I. Alekseev, "Programmno-konfiguriruemye seti kak evoliutsii setevikh tekhnologii [Software-Defined Networks as a Stage of the Network Technology Evolution]," *Modelirovanie i analiz informatsionnykh sistem,* vol. 20, no. 4, pp. 110-124, 2013.

[30] I. Konstantinov, C. J and L. S, “Simulation of the Software-Defined Network for a High-Performance Computing Cluster,” *Research Journal of Appplied Sciences,* vol. 9, no. 10, pp. 704-706, 2014.

[31] D. Chalyy, E. Nikitin and E. Antoshina, “A simple Information Flow Security Model for Software-Define Networks,” *Proceedings of the 17th Conference of Open Innovations Association FRUCT,* pp. 276-282, 2015.

[32] S. Sosenushkin and P. Kruglova, “Adaptivnoe upravlenie resursami informatsionnotelekommunikatsionnoi seti na osnove programmnogo konfigurirovaniia [Adaptive network traffic control based on software defined networking],” *Izvestiia Samarskogo nauchnogo tsentra Rossiiskoi akademii nauk,* vol. 6,

no. 2, pp. 479-484, 2015.

[33] E. Chemeritskii, Issledovanie metodov kontrolia funktsionirovaniia programmno-konfiguriruemykh setei [A study of control methods for monitoring Software-Defined Networks], PhD-Dissertation, Moscow: Moscow State University, 2015.

[34] G. Patrushev, “Servis tsentralizovannoi adaptivnoi marshrutizatsii dlia programmno-konfiguriruemikh setei [Centralized adaptive routing service for Software-Defined Networks],” *12-ia Mezhdunarodnaia Aziatskaia shkola-seminar “Problemy optimizatsii slozhnykh sistem”, Novosibirsk,* pp. 471-478, 2016.

[35] S. Scott-Hayward, G. O'Callaghan and S. Sezer, "SDN Security: A Survey," *2013 Workshop on Software Defined Networks for Future Networks and Services,* Vols. November 11-13, pp. 1-7, 2013.

[36] Cisco, “Block One or More Networks from a BGP Peer,” 2016. [Online]. Available: http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13750-22.html. [Accessed 7 June 2017].

[37] Renesys, “The New Threat: Targeted Internet Traffic Misdirection,” 2013. [Online]. Available: http://dyn.com/blog/mitm-internet-hijacking/. [Accessed 7 June 2017].

[38] SANS, “BGP Hijinks and Hijacks - Incident Response When Your Backbone Is Your Enemy,” 2016. [Online]. Available: https://www.sans.org/reading-room/whitepapers/incident/bgp-hijinks-hijacks-incident-response-backbone-enemy-37422. [Accessed 6 May 2017].

[39] NIST, “Robust Inter-Domain Routing,” 2017. [Online]. Available: https://www.nist.gov/programs-projects/robust-inter-domain-routing. [Accessed 7 June 2017].

[40] R. NCC, “Focus on Russia - RIPE NCC Statistics and Data,” 2017. [Online]. Available: https://labs.ripe.net/Members/fergalc/focus-on-russia-ripe-ncc-statistics-and-data. [Accessed 7 June 2017].

[41] P. Mockapetris, “Domain names - concepts and facilities”. Patent RFC 882, November 1983.

[42] P. Mockapetris, “Domain names - implementation and specification”. Patent RFC 883, November 1983.

[43] P. Mockapetris, “Domain names - concepts and facilities”. Patent RFC 1034, November 1987.

[44] P. Mockapetris, “Domain names - implementation and specification”. Patent RFC 1035, November 1987.

[45] S. Bortzmeyer and S. Huque, “NXDOMAIN: There really is noting underneath”. Patent RFC 8020, 2016.

[46] R. Arends, R. Austein, M. Larson, D. Massey and S. Rose, “DNS Security introduction and requirements”. Patent RFC 4033, March 2005.

[47] P. Hoffmann, “Cryptographic algorithm identifier allocation for DNSSEC”. Patent RFC 6840, November 2010.

[48] S. Weiler and D. Blacka, “Clarifications and implementation notes for DNS security (DNSSEC)”. Patent RFC 6840, 2013.

[49] ICANN, “The problem with 'seven keys',” 2017. [Online]. Available: https://www.icann.org/news/blog/the-problem-with-the-seven-keys. [Accessed 7 June 2017].

[50] D. Kreutz, F. Ramos, P. Veríssimo, C. Rothenberg, S. Azodolmolky and S. Uhlig, “Software-Defined Networking: a Comprehensive Survey,” in *Proceedings of the IEEE, 103 (1)*, 2015.

[51] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, "OpenFlow: Enabling Innovation in Campus Networks," *Computer Communications Review,* vol. 38, no. 2, pp. 69-74, 2008.

[52] J. Sheldon, "The rise of cyberpower," in *Strategy in the Contemporary World*, Oxford, Oxford University Press, 2013, pp. 282-298.

[53] H.-L. Lango, "Competing academic approaches to cyber security," in *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*, New York, Routledge, 2016, pp. 7-26.

[54] J. Barlow, "A Declaration of the Independence in Cyberspace," 1996. [Online]. Available: https://www.eff.org/cyberspace-independence. [Accessed 3 June 2017].

[55] P. Mitchell, "Network Centric Warfare: Coalition operations in the age of US military primacy," IISS, The Alelphi Papers 46:385, 2006.

[56] D. Betz and T. Stevens, "Cyberspace and the State: Toward a Strategy for Cyberpower," Adelphi Series 51:424, 2011.

[57] J. Nye, Cyber Power, Cambridge: Harvard Kennedy School, 2010.

[58] E. Sloan, Modern Military Strategy: An introduction, New York: Routledge, 2012.

[59] R. Slayton, "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security,* vol. 41, no. 3, pp. 72-109, 2016/2017.

[60] N. Pissanidis, H. Rõigas and M. Veenendaal, "8th International Conference on Cyber Conflict (CyCon 2016): Cyber Power, Proceedings," 2016. [Online]. Available: https://ccdcoe.org/cycon/2016/proceedings/CyCon_2016_book.pdf . [Accessed 6 June 2017].

[61] T. Rid, “Cyber war will not take place,” *Journal of Strategic Studies,* vol. 38, no. 1, pp. 5-32, 2012.

[62] J. Stone, “Cyber War Will Take Place!,” *Journal of Strategic Studies,* vol. 36, no. 1, pp. 101-108, 2013.

[63] Tallinn Manual 2.0. On the International Law Applicable to Cyber Operations, Cambridge: Cambridge University Press, 2017.

[64] “United Nations Convention on Cooperation in Combating Information Crimes – an unofficial draft that Russia has presented and distributed for discussion in Commission on Crime Prevention and Criminal Justice,” 2017, May 22-26.

[65] L. Muller, "How to govern cyber security? The limits of the multi-stakeholder approach and the need to rethink public-private cooperation," in *Conflict in Cyber Space. Theoretical, strategic and legal perspectives.*, New York, Routledge, 2016, pp. 116-129.

[66] J. Carr, Inside Cyber Warfare, Sebastopol: O'Reilly, 2012.

[67] T. Rid and B. Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies,* vol. 35, no. 1, pp. 4-37, 2015.

[68] D. Kuehl, “From Cyberspace to Cyberpower - Defining the Problem.,” in *Cyberpower and National Security*, Washington, D.C., National Defence Ubniversity Press, 2009, pp. 24-42.

[69] K. Geers, Strategic Cyber Security, Tallinn: NATO CCD COE, 2011.

[70] T. Rid and P. McBurney, “Cyber-Weapons,” *The RUSI Journal,* vol. 157, no. 1, pp. 6-13, 2012.

[71] J. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security,* vol. 41, no. 3, pp. 44-71, 2016/17.

[72] The Washington Post, “The Sony Pictures hack, explained,” 2014. [Online]. Available: https://www.washingtonpost.com/news/the-

switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.80c976424e7c. [Accessed 3 June 2017].

[73] Reuters, “In cyberattacks such as Sony strike, Obama turns to 'name and shame',” 2015. [Online]. Available: http://www.reuters.com/article/uk-usa-cybersecurity-idUSKBN0KN2E520150114. [Accessed 3 June 2017].

[74] Fireeye, “Redline Drawn: China Recalculates Its Use of Cyber Espionage,” 2016. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

[75] Fifth Domain, “Hackers’ methods feel familiar in Ukraine power grid cyberattack,” 2017. [Online]. Available: http://fifthdomain.com/2017/01/29/how-a-power-grid-got-hacked/. [Accessed 3 June 2017].

[76] CNN, “Intel report: Putin directly ordered effort to influence election,” 2017. [Online]. Available: http://edition.cnn.com/2017/01/06/politics/intelligence-report-putin-election/index.html . [Accessed 3 June 2017].

[77] The Washington Post, “More than 150 countries affected by massive cyberattack, Europol says,” 2017. [Online]. Available: https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html?hpid=hp_hp-more-top-stories_hack-800a%3Ahomepage%2Fstory&utm_term=.78561b84ec9d. [Accessed 3 June 2017].

[78] H. Strachan, The Direction of War: Contemporary Strategy in Historical Perspective, New York: Cambridge University Press, 2013.

[79] L. Freedman, “The Revolution of Strategic Affairs,” the Adelphi

Papers 45:376, 2006.

[80] J. Arquilla and D. Ronfeldt, In Athena’s Camp,, Santa Monica: RAND, 1997.

[81] A. Cebrowski and J. Gartska, “Network-Centric Warfare: Its Origin and Future,” 1998. [Online]. Available: http://www.kinection.com/ncoic/ncw_origin_future.pdf . [Accessed 3 June 2017].

[82] B. Owens, Lifting the Fog of War, Baltimore: The John Hopkins University Press, 2001.

[83] T. Hammes, The Sling and the Stone: On War in the 21st Century, St Paul: Zenith Press, 2006.

[84] J. Chase, “Defining Asymmetric Warfare: A Losing Proposition,” *JFQ ,* vol. 61, pp. 123-126, 2011.

[85] M. Van Creveld, The Transformation of War, New York: The Free Press, 1991.

[86] J. Keegan, A History of Warfare, New York: Vintage Books, 1993.

[87] M. Kaldor, New and Old Wars: Organized Violence in a Global Era, Stanford: Stanford University Press, 2012.

[88] S. Biddle, “The Past as a Prologue: Assessing theories of future warfare,” *Security Studies,* vol. 8, no. 1, pp. 1-74, 1998.

[89] M. Evans, “Elegant irrelevance revisited: A critique of fourth-generation warfare,” *Contemporary Security Policy,* vol. 26, no. 2, pp. 242-249, 2005.

[90] I. Arreguín-Toft, “Contemporary Asymmetric Conflict Theory in Historical Perspective,” *Terrorism and Political Violence,* vol. 24, no. 4, pp. 635-657, 2012.

[91] T. Junio, “Military History and Fourth Generation Warfare,” *Journal of Strategic Studies,* vol. 32, no. 2, pp. 243-269, 2012.

[92] A. Echevarria, “Operational Concepts and Military Strength, 2017 Index of U.S. Military Strength,” 2017. [Online]. Available: http://index.heritage.org/military/2017/essays/operational-concepts-military-strength/ . [Accessed 15 March 2017].

[93] B. Berkowitz, “Chapter seven: Warfare in the Information Age.,” in *In Athena's Camp*, Santa Monica, RAND, 1997, pp. 175-189.

[94] T. Thomas, "Russia 21st Century Information War: Working to Undermine and Destabilize Populations," *Defence Strategic Communications,* vol. 1, no. 1, pp. 11-24, 2015.

[95] F. Kaplan, Dark Territory. The Secret History of Cyber War, New York: Simon & Schuster, 2016.

[96] F. Hoffman, “Hybrid warfare and challenges,” *JFQ,* vol. 52, no. 1st quarter, pp. 34-39, 2009.

[97] B. Renz and H. Smith, “Russia and Hybrid Warfare: Going Beyond the Label, Aleksanteri Papers, 1/2016,,” 2016. [Online]. Available: http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf. [Accessed 6 May 2017].

[98] M. Galeotti, "Heavy Metal Diplomacy: Russia's Political Use of its Military in Europe Since 2014," ECFR, 2016.

[99] V. Gerasimov, “Vystuplenie nachal'nika Genshtaba VS RF generala armii Valeriia Gerasimova na konferentsii MCIS-2016 [The speech of the chief of the General staff of the Russian Armed Forces General Valery Gerasimov at the conference MCIS-2016],” 2017. [Online]. Available: http://mil.ru/mcis/news/more.htm?id=12120704@cmsArticle . [Accessed 8 June 2017].

[100] S. Biddle, “Rebuilding the Foundations of Offense-Defense Theory,” *The Journal of Politics,* vol. 63, no. 3, pp. 741-774, 2001.

[101] D. A. Shlapak and M. W. Johnson, Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of Baltics, Santa Monica: RAND, 2016.

[102] E. Heginbotham, Ed., The U.S. - China Military Scorecard: Forces, Geography, and the Evolution of Balance of Power 1996-2017, Santa Monica: RAND, 2017.

[103] E. Tikk-Ringas, Ed., Evolution of the Cyber Domain: The Implications for National and Global Security, London: The International Institute for Strategic Studies, Routledge, 2015.

[104] CCD COE, “Cyber Security Strategy Documents,” [Online]. Available: https://ccdcoe.org/cyber-security-strategy-documents.html. [Accessed 12 June 2017].

[105] F. Kramer, S. Starr and L. Wentz, Cyberpower and National Security,:, Washington, D.C.: National Defense University Press, 2009.

[106] NATO, “Warsaw Summit Communiqué,” 2016. [Online]. Available: http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber. [Accessed 3 June 2017].

[107] T. Thomas, "Deciphering Asymmetry's Word Game," *Military Review,* no. July-August, pp. 32-37, 2001.

[108] T. Thomas, Russia – Military Strategy: Impacting 21st Century Reform and Geopolitics, Fort Leavenworth: FMSO, 2015.

[109] L. Milevski, “Asymmetry is Strategy, Strategy is Assymmetry,” *JFQ,* vol. 75, no. 4, pp. 77-83, 2014.

[110] J. Angström and J. Widen, Contemporary Military Theory: The

Dynamics of War, New York: Routledge, 2015.

[111] L. Freedman, "Asymmetric Wars," *Adelphi Papers,* vol. 38, no. 318, pp. 33-48, 1998.

[112] E. Gartzke and J. Lindsay, "Cross-Domain Deterrence: Strategy in an Era of Complexity," 2014. [Online]. Available: https://quote.ucsd.edu/deterrence/files/2014/12/EGLindsay_CDD Overview_20140715.pdf.. [Accessed 3 June 2017].

[113] J. Boyd, "The Essence of Winning and Losing," 1996. [Online]. Available: https://fasttransients.files.wordpress.com/2010/03/essence_of_winning_losing.pdf. [Accessed 3 June 2017].

[114] J. Hanska, Times of War and War over Time: The roles time and timing play in operational art and its development according to the texts of renowned theorists and practitioners, Helsinki: National Defence University, 2017.

[115] M. W. Svolik, The Politics of Authoritarian Rule, New York: Cambridge University Pres, 2012.

[116] M. Dutta, "A Review of Automated Intrusion Detection Models," *International Research Journal of Engineering and Technology (IRJET),* vol. 3, no. 5, pp. 1980-1983, 2016.

[117] L. Aron, "The Problematic Pages, New Republic, September 24, 2008," 2008. [Online]. Available: https://newrepublic.com/article/62070/the-problematic-pages. [Accessed 6 June 2017].

[118] S. Blank, "Threats to and from Russia: An Assessment," *The Journal of Slavic Military Studies,* vol. 21, no. 3, pp. 491-526, 2008.

[119] A. Monaghan, "'An enemy at the gates' of 'from victory to victory'?," *Russian foreign policy, International Affairs,* vol. 84,

no. 4, pp. 717-733, 2008.

[120] J. Mearsheimer, “Getting Ukraine Wrong,” 2014. [Online]. Available: https://www.nytimes.com/2014/03/14/opinion/getting-ukraine-wrong.html?_r=0). [Accessed 6 June 2017].

[121] R. Sakwa, “The Deep Rootsof the Ukraine Crisis – To Forge a Lasting Peace in Europe, We Must Rethink the Post-Cold War Security Order,” *The Nation,* vol. 300, no. 18, pp. 30-32, 2015.

[122] S. Walt, “Who is a Better Strategist: Obama or Putin?,” *Foreign Policy,* 15 October 2015.

[123] H. Guerlac, “Vauban: The Impact of Science of War,” in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, Oxford, Clarendon Press, 1990, pp. 64-90.

[124] I. Panarin and L. Panarina, Informatsionnaia voina i mir. Informatsionnoe protivoborstvo v sovremennom mire [Information War and Peace. Information Counter Struggle in the Contemporary World], Moskva: OLMA-PRESS, 2003.

[125] N. Choucri, Cyberpolitics in International Relations, Cambridge: MIT Press, 2012.

[126] A. V. Manoilo, Gosudarstvennaia informatsionnaia politika v osobykh usloviiakh [State Information Policy in Special Circumstances], Moskva: MIFI, 2003.

[127] NATO, “Comprehensive Operations Planning Directive COPD V2.0, 04 October 2013,” 2013. [Online]. Available: www.act.nato.int/images/stories/events/2014/sfpdpe/copd_v20.pdf . [Accessed 20 March 2017].

[128] T. Thomas, "Thinking Like a Russian Officer: Basic Factors And Contemporary Thinking On The Nature of War," January-March 2016. [Online]. [Accessed 2 March 2017].

[129] RuBroad.ru, “Top-10 magistral’nyk provaiderov Rossii i Top-3 krupneishikh magistral’nykh provaiderov Moskvy, 10.2.2014 [Top 10 backbone providers in Russia and Top-3 the largest backbone providers in Moscow, 10.2.2014],” 2014. [Online]. Available: http://rubroad.ru/magazine/providers/4530-top- . [Accessed 9 June 2017].

[130] “Provy.ru,” 2017. [Online]. Available: http://russia.provy.ru/providers. [Accessed 9 June 2017].

[131] “MSK-IX,” 2017. [Online]. Available: https://www.msk-ix.ru/company/ . [Accessed 9 June 2017].

[132] “DATAIX,” 2017. [Online]. Available: http://dataix.ru/partnership/. [Accessed 9 June 2017].

[133] “Root-servers.org,” 2017. [Online]. Available: http://www.root-servers.org/ . [Accessed 9 June 2017].

[134] “Russian Federation - Official Russia: Information on RSNet Administration,” [Online]. Available: http://www.gov.ru/main/rsnet/page541.html. [Accessed 9 June 2017].

[135] V. Zykov and A. Ramm, “V Rossii poiavilsia voennyi internet [A military internet appeared in Russia],” *Izvestiia,* 19 October 2016.

[136] “Federalnyi zakon: O sviazi, 07.07.2003, No. 126-FZ (poslednaia redaktsiia ot 17.04.2017, No. 75-FZ), [Federal Law On connections 07.07.2003, No. 126-FZ (last updated 17.04.2017, No. 75-FZ)],” 2017. [Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=215565&fld=134&dst=1000000001,0&rnd=0.4256394509185802#0. [Accessed 9 June 2017].

[137] K. Ermoshina and F. Musiani, “Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era,” *Media and Communication,* vol. 5, no. 1, pp. 42-53, 2017.

[138] "Yandex.ru: Razvitie interneta v regionakh Rossii [Regional development of the Internet in Russia]," 2016. [Online]. Available: https://yandex.ru/company/researches/2016/ya_internet_regions_2016. [Accessed 9 June 2017].

[139] "Internet Live Stats: Russia Internet Users," 2017. [Online]. Available: http://www.internetlivestats.com/internet-users/russia/. [Accessed 9 June 2017].

[140] H. Simon, The New Science of Management Decision, NJ: Englewood Cliffs, Prentice Hall, 1977.

[141] D. Kulick and M. Egner, Implications of Modern Decision Science on Military Decision Support Systems, Santa Monica: RAND, 2015.

[142] J. Godwin III, A. Kulpim, K. Rauscher and V. Yaschenko, Eds., Critical terminology foundations 2. Russia-U.S. Bilateral on Cybersecurity. Policy Report 2/2014, EastWest Institute and the Information Security Institute of Moscow State University, 2014.

[143] United State Department of Defence (U.S. DoD), "Joint Publication 3-0: Joint Operations," 17 January 2017. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf. [Accessed 20 August 2017].

Modelling the imbalance of cyber operations between closed and open national networks

Juha Kukkola
Vesa Kuikka
Juha-Pekka Nikkarila

Abstract

We introduce a mathematical model to describe asymmetric frontlines that are formed if a nation closes their national networks. When considering defence, the model gives the capability as a probability for denying adversarial operation in a friendly network. The closing process is a well-documented course of development as Russia is likely to implement RuNet 2020. The model may be used to form and improve situation awareness as the process evolves.

Keywords: Modelling military capability, Battlefield of the future, Cyber domain, Closed network nation, Asymmetric frontlines, RuNet

This extended abstract was published and presented at the annual conference of the International Society for Military Sciences (ISMS 2017), Oslo, Norway, November 15–17, 2017.

1 Introduction

We propose a model to describe the change in capability caused by asymmetric frontlines between closed and open national networks. The capability is presented as a probability for denying adversarial operations in a friendly network. In summer 2016, almost at the same time as NATO recognized cyberspace as a military domain, Russia declared that RuNet – the Russian segment of the Internet – would be disconnected from the global Internet by 2020 [1]. The de facto process of closing national networks is referred to as a closing process. We have continued research in order to improve situation awareness of the closing process, analysed its military aims and impacts. We have deduced that the military motivation behind Russia's network closing process is related to improving its military capabilities in cyberspace, namely traditional elements of combat power: protection, (relative) maneuverability and (relative) firepower. Hence, the motive behind a closed network nation is to achieve higher operational capability than an ‘open network society’. On the other hand, the motive for introducing RuNet may also be related to challenging the current world order.

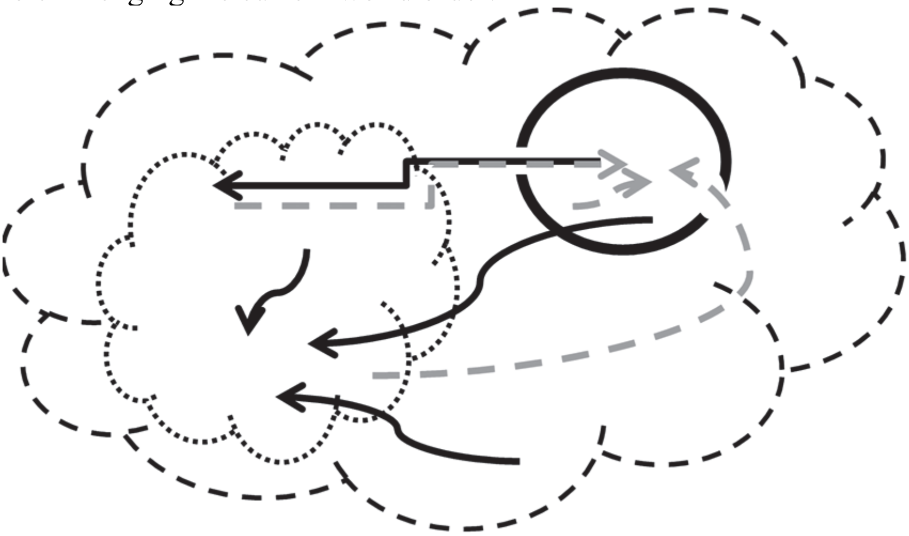


Figure 1.1: Schematic outline of open society network’s asymmetry to a closed national network. The closed network is presented by a solid lined eclipse on the right and is enclosed by an open network society (i.e. the Internet). The dotted cloud represents an open national network (figure from [3]).

2 Potential impact of the closing process

We have analyzed the outcomes of closing process from an open network society’s perspective and shown how a closed network nation is able to shape the cyber domain. The purpose of shaping the cyber domain is to gain an advantage and consequently, to control the cyber domain. There is a danger of open network societies being forced into a reactive mode. In our earlier study, we analysed the choices facing open network societies and their consequences in the case of escalation and even potential confrontation [3].

Maybe one of the most interesting results of the closing process is the formation of asymmetric frontlines in the cyber domain. In the paper we discuss how the fragmentation of global network is progressing towards the formation of national segments of cyberspace. These national segments will be walled with ‘digital borders’ and will enforce the concept of digital sovereignty; e.g. by closing their national networks. In the earlier study, we argue how the conventional asymmetry in cyberspace originates from the problem of attribution, and is challenged or even made obsolete by the concept of digital sovereignty. We demonstrated how 'digital sovereignty' is achievable by innovatively applying current technology and protocols. There is an obvious impact of the digital sovereignty and the resulting asymmetric frontlines to the (near) future cyber battlefields [4].

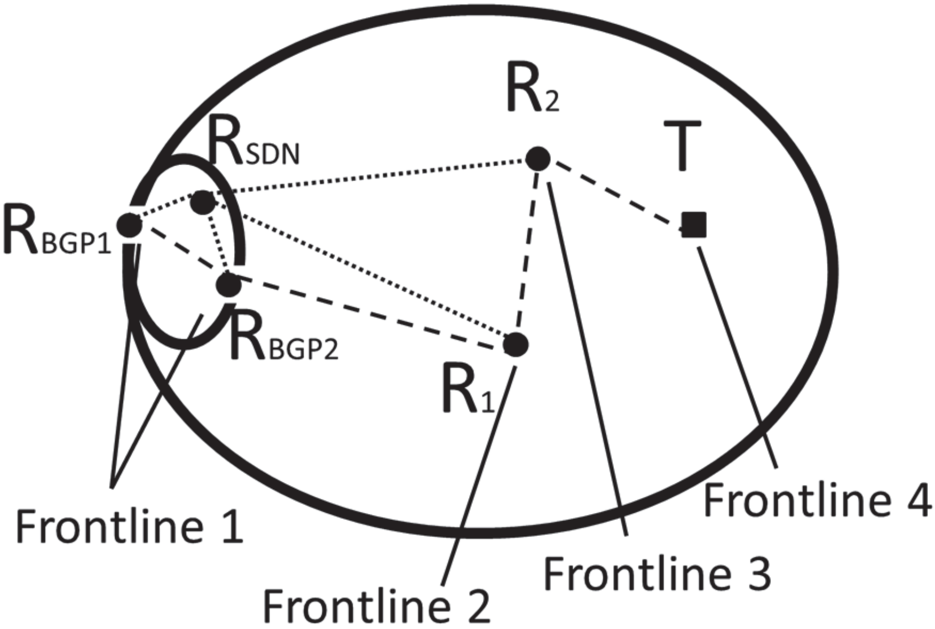


Figure 2.1: A simplified outline of the frontlines of a closed network. The largest ellipse represents the closed subspace and the smaller one demonstrates the 'border crossing-point' and 'digital customs' (cf. Streltsov & Pilyugin 2016) between the open subspace and the closed subspace. Since similar frontlines are absent in the open network it results in asymmetric frontlines. In the open national network all the safety measures are essentially conducted within or at the borders of the specific IT-system (marked as T=target in the figure). In the figure, one decision making router RSDN is actually a set of several routers that may be centrally controlled (Figure from [4]).

Obviously there is a need for more specific research on this subject. We reviewed our previous studies in a NATO IST-145 publication [5] pertaining to adversarial cyber operations aiming to the fragmentation of the global network. The motivation for writing the review article was to address the network closure process and its potential impacts on the open network society. We would like to guide the resources of the scientific community to work further with this problem.

There is a need for mathematical, technological and military research for considering the network closing problem. In the current research we provide mathematical analysis considering the problem related to closed national networks. The proposed model presents a probability based view of the military capability of closed and open networks.

3 Probabilistic model

Probabilistic models of war have been proposed in the literature [6], [7]. In this paper we use conditional probabilities to model asymmetric cyber-attacks and defence between closed and open national networks. The method is based on our earlier work on technology forecasting and capability modelling [8], [9], [10], [11].

Military capabilities can be modeled with basic probability theory using conditional probabilities. Our modelling is based on a system of systems concept, where a system can be described as parallel and serial sub-systems with a desired granularity. The highest level of modeling can be comprised of capability areas or a subset of functionalities from one or more capability area. Functionalities are assumed to be independent – and if this does not hold, they should be further separated until the functionalities have no interceptions.

The general idea is to model the operation as multiple phases or levels. Typically, two taxonomies exist for the classification of attacks and defence actions. These two taxonomies may have common functionalities but usually the probabilities of sucess are different depending on the scenarios and other environmental factors [12], [13].

In our first schematic model we have a structure for functionalities where inner levels are conditional to all outer levels of action. In a general form we express the model mathematically for the probability of successful operation as follows:

$$P=1-(1-p_1\,|\,0)(1-p_2\,|\,0\wedge 1)(1-p_3\,|\,0\wedge 1\wedge 2)\cdots(1-p_n\,|\,0\wedge 1\wedge 2..n-1), \quad (1)$$

where $p_i, i = 1,...,n$ describe the probabilities of success in *n* tasks. These tasks or sub-functionalities together describe an operation. The nested structure shows up with the conditional probabilities denoted by $0, 0 \wedge 1, ..., 0 \wedge 1 \wedge 2 ... n-1$. Conditional probability is a measure of the probability of an event given that another event has occurred, for example, $p_2 \mid 0 \wedge 1$ is the probability of successfully carring out a second task given that tasks or events *i*=0 and *i*=1 have happened. The event *i*=0 is the presumption that the operation occurs at all.

In the following, we use the short hand notation $p_i = p_i \mid 0 \wedge 1 .. i-1$. If at any level $i = 1, ..., n$, alternative systems or operational procedures exist, the formula is modified accordingly. For example, the probability for task *i* having *j* alternatives is

$$p_i = 1 - (1 - p_{i,1})(1 - p_{i,2}) \cdots (1 - p_{i,j})$$

If at any level $i = 1, ..., n$, multiple functionalities are necessary for a successful task *i*, the probability is

$$p_i = p_{i,1} p_{i,2} \cdots p_{i,j} \, .$$

The idea is generalized for sub-level functionalities and at the same level both alternative and necessary structures may exist.

As an example, we describe a defensive operation (from a closed national network perspective):

$$P_{defense} = 1 - (1 - p_{Deny\,\mathrm{Re}connaisance})(1 - p_{Deny\,Unauthorized\,BC})(1 - p_{Deny\,Adavancement})(1 - p_{Deny\,Cyber\,Attack}), \quad (2)$$

where $p_{Deny\,\mathrm{Re}connaisance}$ stands for the probability of denying reconnaissance, $p_{Deny\,Unauthoriz\,ed\,BC}$ unauthorized border crossing, $p_{Deny\,Adavancement}$ denying adversarial advancement within the closed networks and $p_{Deny\,Cyber\,Attack}$ denying cyber-attack on or within the system itself.

The description for a corresponding cyber-attack operation is then:

$$
\begin{aligned}
P_{attack} &= p_{\mathrm{Reconnaissance}}\, p_{BorderCrossing}\, p_{Advancement}\, p_{Cyber\,Attack} \\
&= \left(1 - p_{Deny\mathrm{Reconnaisance}}\right)\left(1 - p_{DenyUnauthorized\,BC}\right)\left(1 - p_{DenyAdavancement}\right)\left(1 - p_{DenyCyberAttack}\right)
\end{aligned}
. \quad (3)
$$

$$
\boxed{\begin{aligned}&\mathrm{Capability}=1-(1-P_1)(1-P_2\ )(1-P_3)(1-P_4)= \\ &P_1+(1-P_1)P_2+(1-P_1)(1-P_2)P_3+(1-P_1)(1-P_2)(1-P_3)P_4\end{aligned}}
$$

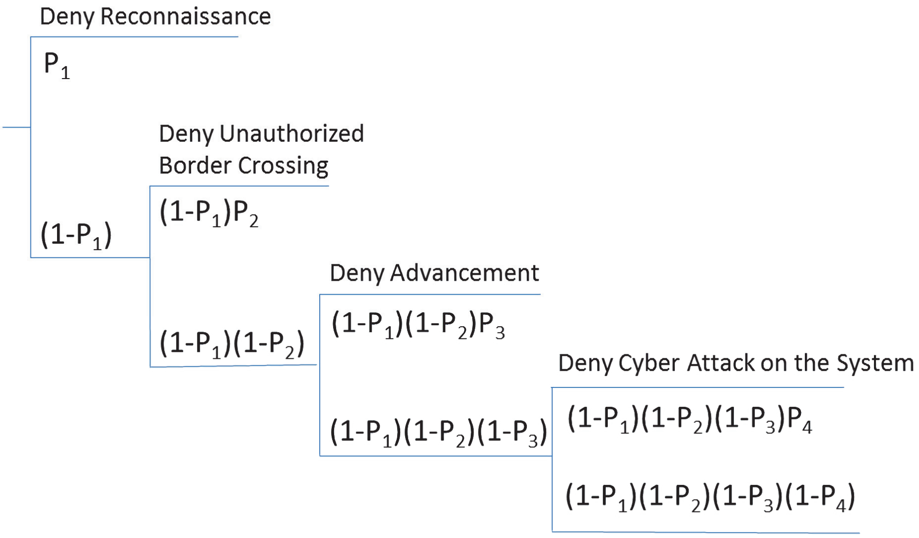

Deny Reconnaissance
P_1
$(1-P_1)$
Deny Unauthorized Border Crossing
$(1-P_1)P_2$
$(1-P_1)(1-P_2)$
Deny Advancement
$(1-P_1)(1-P_2)P_3$
$(1-P_1)(1-P_2)(1-P_3)$
Deny Cyber Attack on the System
$(1-P_1)(1-P_2)(1-P_3)P_4$
$(1-P_1)(1-P_2)(1-P_3)(1-P_4)$

Figure 3.1: Illustration of a defensive operation (from a closed network perspective) for Equation (2).

When a cyber operation is conducted in the other direction, namely from the closed network toward open national networks, similar frontlines do not exist (by definition). This has been discussed in our earlier research [4] and the outcome is the formation of asymmetric frontlines.

4 Conclusion

We have presented, to the best of our knowledge, the first mathematical model to describe the imbalance of cyber operations between closed and open national networks. The effect on the military capabilities of the closed and open networks has been analysed with the model. The closing process is a well-documented course of development and will be de facto in 2020 as Russia is likely to implement RuNet 2020. As the closing process continues the understanding of it needs to progress as well. We are further developing the model and also otherwise constructing situation awareness of the process. We encourage the scientific community in general to further study the problem.

References

[1] Ristolainen, M., Should ‘RuNet 2020’ be taken seriously?, in ECCWS, In Press 2017.

[2] Nikkarila, J.-P., and Ristolainen, M., “‘RuNet 2020’ - Deploying traditional elements of combat power in cyberspace?,” in ICMCIS, 2017.

[3] Kukkola, J., Ristolainen, M., Nikkarila, J.-P., Confrontation with Closed Network Nation Open Network Society’s Choices and Consequences, in MILCOM, 2017a.

[4] Kukkola, J., Nikkarila, J.-P., Ristolainen, M., ‘Asymmetric frontlines’ of the cyber battlefields, in ICCRTS, 2017b.

[5] Kukkola, J., Nikkarila, J.-P., Ristolainen, M., Shaping Cyberspace: A predictive analysis of adversarial cyber capabilities, in IST-145/RSM-030 Specialists’ Meeting on Predictive Analytics and Analysis in the Cyber Domain, 2017c.

[6] Cioffi-Revilla, C., Mathematical contributions to the scientific understanding of war, Mathematical and Computer Modelling, Vol. 12, Issues 4–5, Pages 561-575, 1989.

[7] Cioffi-Revilla, C., Dacey, R., The probability of war in then-crises problem: Modeling new alternatives to Wright’s solution, Synthese, Volume 76, Issue 2, pp 285–305, August 1988.

[8] Kuikka, V., Suojanen, M., Modeling the Impact of Technologies and Systems on Military Capabilities, Journal of Battlefield Technology, Vol. 17, No. 2, 9-16, 2014.

[9] Kuikka, V., Nikkarila, J-P., Suojanen, M., A Technology Forecasting Method for Capabilities of a System of Systems, PICMET Conference, 2015a.

[10] Kuikka, V., Nikkarila, J-P., Suojanen, M. , Dependency of Military Capabilities on Technological Development, Journal of Military Studies, Vol 6, No 2, 2015b.

[11] Kuikka, V., Number of system units optimizing the capability requirements through multiple system capabilities, Journal of Applied Operational Research, Vol. 8, No. 1, 26–41, 2016.

[12] Suojanen M., Kuikka, V., Nikkarila, J-P., Nurmi, J., An Example of Scenario-based Evaluation of Military Capability Areas – An Impact Assessment of Alternative Systems on Operations, IEEE International Systems Conference, 2015.

[13] Kukkola, J., Ristolainen, M., Russian Conceptual Control of the Cyber Domain: The Five Basic Principles of War, poster presented in ECCWS, 2017.

Cyber asymmetry
– Towards new strategic thinking?

Juha Kukkola

Abstract

The paper argues that traditional Western views of asymmetry are hindering our understanding of military strategic issues in cyberspace. These views suffer from a kind of (Western) cultural bias, an artificial dichotomy between offense and defence, and the basic flaw of forgetting the 'dialectic of force'. In this paper it is argued that the effort of some states to create digital sovereignty in cyberspace is in fact an intentional project to create a strategic asymmetric advantage. This advantage is both defensive and offensive. By shaping and delineating cyberspace with technical, administrative and political tools and creating closed national Internets, states achieve a relative advantage in situation awareness, freedom of action, protection of assets and speed of decision making. This asymmetry gives these states a definite advantage on a strategic level vis-à-vis nations who decide to rely on a free and open Internet. To understand how 'digital sovereignty' creates cyber asymmetry it is necessary to revise concepts of cyber power and asymmetry. By examining traditional uses of cyber power and asymmetry, this paper proposes concepts that are more contextual, relational, cultural and structural than previous ones. From these concepts it is possible to develop tools for further analysis of cyber asymmetry created by the intentional closing of national cyberspace. Overall the paper aims to challenge traditional Western views on asymmetry especially in cyberspace and enhance our understanding of some of the strategic processes threatening the Internet as we know it today.

Keywords: Cyber power, Cyberspace, Structural Cyber Asymmetry, Digital Sovereignty, Closed National Network

1 Introduction

The Russian Federation and to a lesser extent the Republic of China have been increasing their control of the national portion of the Internet. At the same time international efforts to create common norms for the Internet are faltering [1]. It seems, that the open, safe and secure Internet is facing a challenge from territorially minded nation states [2], [3], [4], [5] [6, pp.

31-41]. The challenge rises partly from political and economic considerations, but there is also a military aspect behind plans to control the Internet and maybe close national parts of it from wider cyberspace [7], [2], [8], [9]. This is directly related to cyberspace's possible role as domain of warfare in intrastate conflicts [10].

This paper develops an argument presented previously that nations supporting a free, open and secure Internet maybe facing an asymmetrical threat in cyberspace in the near future [2], [11], [8], [9]. Western[1] nations in particular are too attached to viewing asymmetrical threats as related to non-state actors and there is an artificial separation between strategic offensive and defensive actions. Emerging security strategies are focused on critical infrastructure and psychological aspects of information warfare.[23] Additionally, offensive doctrines are limited to distinguishable conflicts on tactical or operational levels and are basically reactive in their nature [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22]. Strategic thinking is centred upon deterrence or operations, not on preparing for cyber warfare as a whole [23], [24], [18]. At the same time, a more holistic view is taken by Russia which sees itself in a continuous struggle with the West and combines offensive and defensive strategies more flexibly [25], [26]. In this situation strategies understood as planning and conducting operations do not work. The West must relearn what André Beaufe meant by the 'dialectic of force', and it does not get to choose and control the battlefield anymore (On Beaufe see [27]).

[1] In this paper the term West or Western refers to a political and value based group of nations centred on the United States and its allies. These states are mainly members of the same international institutions (particularly NATO), and share similar political systems (democracy), values (rule of law, freedom of speech etc.) and economic systems (a market or mixed economy). The Non-West is characterised by differing institutions (Collective Security Treaty Organisation etc.), political systems (authoritarianism etc.), values (fundamental religious law system etc.) and economic systems (state capitalism etc.)

[2] On the development of threat perception against critical infrastructure in the United States, cf. [149]; Efforts to combat violent extremism after the 9/11 terrorist attacks and failures in Iraq and Afghanistan underlined the need for 'Strategic Communications' (influencing selected audiences in support of national objectives) [150]. After the rise of the Islamic State (ISIS/ISIL) the focus was shifted to counter recruitment information operations, in which social media had an important role. Then the focus shifted again to Russia's information operations which allegedly targeted Western norms and political systems, mainly through Internet-enabled news services, social media and hacking [151].

[3] Information warfare is used here in lower case because the concept is essentially contested and ambiguous [152, pp. 508-510], [153]. It is used in this paper as a higher-level concept, denoting the use of information for military strategic aims in peace or wartime.

The concept of military asymmetry has been connected to non-state actors using nation state vulnerabilities and, on other hand, to the inefficiency of deterrence against these non-state actors.[4] This view is too narrow, culturally bound to Western military thought, concentrates on only a few aspects of asymmetry and does not take into account the fact that cyberspace, unlike other domains of warfare, can be shaped on a strategic level. As Kukkola, Ristolainen and Nikkarila have previously argued, by using technical, administrative and political means, states can create asymmetries, which in effect create power based on structural changes of cyberspace [9]. This asymmetry can be called 'structural cyber asymmetry' and it can be considered a product of the territorialisation of the Internet [28].

The structural concept of asymmetry is not altogether speculative. The Russian Federation is already creating a basis for this with its idea of 'digital sovereignty' [2]. In short, this means state control of territorial cyberspace including physical, syntactic, and semantic levels, and in the extreme this also includes the ability to close the national Internet from the global network. This would give Russia both defensive and offensive advantages in cyberspace. States have differing ideas on cyber warfare and Russia's case is a good example of how strategic culture[5] affects national understandings of cyber power, cyberspace and warfare. It is argued that these understandings have real life effects in how cyberspace is shaped by state actors.

The aim of this paper is to further conceptualise cyber asymmetry as creating and exploiting structural advantages by shaping cyberspace. The paper starts with an introduction and then continues to the methodology. In the third part the paper proceeds to discuss cyberspace and cyber power, and in particular cyber power's military aspects and shaping function. A modified neoclassical realist approach is used to argue that strategic thinking is affected by culture and that understandings about cyber issues are contextually and culturally bound.[6] In the fourth part, the paper examines the conceptual history of asymmetry in warfare to show how its main version is based on a certain kind of understanding of warfare and how there are alternative ways to understand it. A new version of cyber asymmetry is then formulated. In the fifth part, conclusions are presented and discussion is offered on future research.

[4] See chapter 4.

[5] See chapter 3 on strategic culture.

[6] Time and place, policy issue under consideration, and beliefs and preferences that state elites hold affect how they understand and act on cyber issues. On strategic culture, cf. [41].

2 Methods and materials

This paper combines theories, methods and materials from international relations (IR) [29] and security and strategic studies [30]. Specifically, it also refers to material from the fields of Russian studies and cyber studies. The paper starts by presenting a theoretical framework for the study. Then a historical literature survey of central concepts is conducted, and using conceptual analysis, the concepts of ‘cyberspace’, ‘cyber power’ and ‘structural cyber asymmetry’ are reformulated to fit the framework. As a result of the conceptual part of the paper, ‘structural cyber asymmetry’ is operationalised for the study of ideas, policies and structures.

The research material consists of previous IR, political science, military and cyber studies and reports and strategies on cyber security and defence. These sources are used to examine how understandings on power, asymmetry and cyber issues have evolved, and how they might contribute to forming a new concept.

3 Cyberspace and cyber power

In this chapter it is argued that power is first and foremost a relational and contextual concept. A framework based on neoclassical realism and the study of strategic cultures is offered as a basis for understanding cyberspace and cyber power in a political-strategic context. From this theoretical viewpoint it is possible to form the concept of cyber power that supports the concept of ‘structural cyber asymmetry.’

It should be pointed out that the concepts and theories discussed in this chapter are based on English speaking academic discourses. There are three reasons for this. Firstly, the main concepts and theories examined in this study have been developed in English speaking media, academia and governmental institutions. Secondly, these concepts present a somewhat coherent and established framework for the study of cyber issues. Thirdly, and most importantly, this approach allows comparisons with concepts and theories from other cultural contexts. With this in mind, ‘structural cyber asymmetry’ is a description of an object, which might be understood, created and used differently by different states, but still has objective, independent effects. A nuclear bomb is still a nuclear bomb, and a router is still a router whatever we might think of them.

3.1 Neoclassical realism

This paper adopts neoclassical realism for its loose theoretical framework, which is a school of international relations (IR).[7] It is the latest incarnation of the so-called realist school and an attempt to answer questions raised by constructivists in IR studies. The school of thought does not have a single theory, but for the sake of clarity, the term theory is used in this paper [31]. Basically, neoclassical realist theory states that the international system is anarchy and states can rely only on self-help to achieve security. Neoclassical theory differs from earlier realist schools in that it is basically a theory of foreign policy. It accepts both system and unit level variables and it allows for the perceptions of decision makers and domestic politics to affect state behavior. These ideas come together in a term ‘transmission belt’ which is a concept describing how national power resources are converted to state power on the international level [31]. In the context of this paper it is important to note that according to Gideon Rose, neoclassical realists tend to see power as ‘material’, not ‘relational’ because studying the balance of power from outcomes is ‘dubious’ [32, p. 151]. Be that as it may, the theory in effect allows the study of how perceptions, culture, domestic politics, public opinion and institutions affect a state’s foreign policy. This means that power has to be analysed from the point of view of decision makers. So, decision making elites are in a key position here. Their behavior is restricted and enabled partly by their understanding of the international system, domestic variables and the culture they are part of [32, pp. 146-148], [33, pp. 315-318]. Lobell et al. [31, p. 20] summarises the underlying causal logic as follows: relative power distributions are independent variables, domestic constrains and elite perceptions are intervening variables and foreign policy is a dependent variable.

Neoclassical realism has been criticised for trying to fix neorealism (i.e. answer the question why states do not behave according to a systemic balance-of-power) by introducing unit level variables and in that effort

[7] The term ‘neoclassical realism’ was coined by Gideon Rose [32, p. 146] in a review article. He states that: “It explicitly incorporates both external and internal variables, updating and systematising certain insights drawn from classical realist thought. Its adherents argue that the scope and ambition of a country’s foreign policy is driven first and foremost by its place in the international system and specifically by its relative material power capabilities. This is why they are realists. They argue further, however, that the impact of such power capabilities on foreign policy is indirect and complex, because systemic pressures must be translated through intervening variables at the unit level. This is why they are neoclassical.”

sacrifice the last vestiges of parsimony there ever was in realist theory.[8] Brian Rathburn counters this by arguing that neoclassical realism is in fact meant to study situations when "decision making is impaired by uncertainty and the complexity of the environment" [33, p. 295] and Lobell et al. defend neoclassical realism by arguing that it is an independent theory from neorealism. Nevertheless, accepting ideational variables has left neoclassical realism with difficulties to distinguish itself from another IR theory, constructivism, which sees ideas, identities and interests as causal or constitutive variables.[9] The main difference may be that realism argues for an objective material reality that (in the end) constrains actions, whereas constructivists deny this and see socially construed meanings as constraints and view all meaning as changeable [33, p. 319]. There are also differences within neoclassical realism on the importance of international system level variables (balance-of-power), rationality of decision making elites and on the relationship between ideas and matter (cf. [34], [35]). This ambivalence in ontology, epistemology and methodology is not particular to neoclassical realism but is a larger issue within IR.[10]

In the context of this paper, the theoretical problems of neoclassical realism are secondary. It is not used to derive hypotheses. The theory provides a framework for understanding international relations (systems of states) and state behavior (non-unitary actors) and allows context and perceptions (culture), in addition to resources and systemic constrains, to affect how power is utilised. As is shown below, this paper takes a broader approach to culture than more mainstream interpretations of neoclassical realism, because it permits the concept of strategic culture to play a more definite role in shaping ideas and the behavior of decision makers. Furthermore, neoclassical realism's view on power is too narrow, but basically appropriate in stating that its resources and effects are real. However, power is relational and contextual. How decision makers understand the utility of power is important for studying the *ways* power is used.[11] Strategic culture plays an important role in this.

3.2 Strategic culture

Strategic studies is an interdisciplinary field of study that was developed during the Cold War [30, pp. 1-6]. Its main focus is the study of use of

[8] For criticism of neoclassical realism see [154].

[9] On constructivism see [155].

[10] Philosophy of science in international relations is not a clearly defined [156].

[11] See Chapter 3 on power

force from theoretical and practical perspectives [36, pp. 17-22], [37, p. 123], [38, p. x]. It has a close, and somewhat strained, relationship with security studies[12], which takes a broader and more critical view of security issues [39, p. 41], [40, p. 359]. Strategic culture is a concept developed in the context of strategic studies in 1977 by Jack Snyder. He described it as: "a set of beliefs, attitudes, and behavior patterns with regard to nuclear strategy that has achieved a state of semi-permanence that places them on the level of "cultural" rather than mere policy." [41, p. 87] . The basic idea is that there may be a national, somewhat stable way to think about military strategic issues and this may have an effect on state preferences and behavior [37, p. 131]. The concept of strategic culture has been more or less connected to realist IR theory and strategic studies in particular and has gone through a similar epistemological and ontological development as neoclassical realism. There have been at least three waves of theories on strategic culture after Snyder's work. Lantis and Howlett [41] describe these approaches as value adding, explanatory and immersive, the distinction being what kind of explanatory power is given to culture. Doeser [42] describes the same phenomenon as an intermediate filtering variable, independent causal variable and constitutive structure [42, p. 285]. Colin Gray has this to say on strategic culture: "On the contrary [to rational choice] when security communities exercise strategic choice they do so not with a completely open, or blank, mind on strategic ideas, but rather with values, attitudes, and preferences through which they filter new data, and in terms of which they judge among alternative courses of action," [37, p. 29]. Gray proposes that the effect of strategic culture is empirical question and can be answered by observing behavior of states [37, p. 136]. Whatever the effect of strategic culture, it seems that elites, mainly military and security establishments are the main carriers of strategic culture, but are not free to manipulate culture at their will [37, pp. 87-88], [42, p. 286]. It is also important to note that strategic culture is not a theory but a concept with different interpretations depending on the research agenda.

The main problem of strategic culture is that it is difficult to operationalise. Causality of culture is difficult to prove. The second problem is change. It is difficult, on the one hand, to point out when cultures change because of outside effects or interaction with other cultures and, on the other hand, when they are intentionally changed or manipulated [41, pp. 91-95]. For example, Hew Strachan has criticised strategic culture for overemphasising continuity, and because of this, it is

[12] Lower cases are used here to express the broad field of different approaches, cf. [40, p. 359].

unable to predict the future [39, pp. 136-140]. The so called ‘third generation’ has responded to this criticism by adopting a more constructive approach, by concentrating on particular cases and proposing that there could be more than one monolithic strategic culture in a security community [43, pp. 78-81]. As one of the representatives of the ‘first generation’ Colin Gray has tried to form a synthesis of generations by proposing a synthesis of context and behavior. Strategic culture gives meaning to observed reality and is observable in behavior [43, pp. 80-81].

From the point of view of this paper, strategic culture is a beneficial concept, because it describes one of the intervening variables of the neoclassical transmission belt and allows us to argue that states can have different understandings of cyber power and cyberspace. There is an objective, material reality but how this is understood and how the use of force is comprehended and then utilised differs between states. This is especially true concerning new situations and new methods cf. [36], [44], [45], [46]. In sum, this paper takes a slightly more constructivist approach to neoclassical realism and strategic culture than may be good for the principle of parsimony and coherence of neoclassical realist theory. This is justifiable, because the aim of this paper is not to construct conceptual apparatus for the study of causal relationships, but to explore descriptive and explanative power of one particular concept (‘structural cyber asymmetry’). Culture has to be seen as an immersive or cultural structure – as something that gives meaning to all of observed reality and guides behavior, but does not control it. In this respect culture cannot be seen as an unchangeable and monolithic structure [37, p. 131]. There are subcultures inside elites, and there are cultures outside the state that it can adapt to [41, pp. 85-88]. Because cyberspace and cyber power are relatively new and contested phenomena in a political-strategic context the theoretical framework proposed here is a suitable approach.[13]

3.3 Cyberspace

Strategic thinking about cyberspace and cyber power started in the 1990s but really got off the ground at the beginning of 2000s [47], [48], [49], [7], [50]. Concepts and theories have not yet matured enough that the term ‘scientific’ theory could be used and many of the concepts are academically and politically contested [51, pp. 21-22]. This observation, of course, argues for the neoclassical realist and cultural approach adopted in this paper. Consequently, because power is a contextual and relational phenomenon [52, p. 275], the analysis must start from space.

[13] On contested nature see [10].

According to John B. Sheldon the term cyberspace was coined by science-fiction writer William Gibson in 1982 [53, p. 304]. Gibson has described the term as initially empty of any meaning [54], which he then defined as "'consensual hallucination' that takes place when humans interact with networked computers" [53, p. 304]. The prefix to space used by Gibson has its roots in 'cybernetics' which was developed by mathematician Norbert Wiener 1948. He was interested in human machine interfaces, control and feedback mechanisms, and borrowed the term cyber from Greek (*steerman*) [55, p. 17]. Cybernetics had a great impact on the development of robotics, computers and networks during the Cold War on both sides of the confrontation [56]. It was adopted by Soviet scientists as *kibernetika* which expanded later to encompass a large part of the Soviet scientific field. It was replaced in the 1980s by '*informatika*' which can be translated as computer science [55, p. 48]. In the West the cyber term transformed gradually during the 1990s to mean almost anything related to networks and computers [50, p. 46], [56, pp. 303-307]. Based on this short terminological history it can be argued that the meanings of cyberspace and power are cultural and contextual. What is even more interesting is that there has been transfer of ideas between hostile cultures. With this in mind, this paper uses the term cyber as a prefix that takes its meaning in combination with other terms. Brandon Valeriano and Ryan C. Maness have described cyber as meaning 'computer and digital interactions' [51, p. 22]. It seems to resonate adequately with both Western and Russian concepts.

In the Western cyber literature there are numerous definitions for cyberspace. The definitions depend on the agenda behind them. Only those that have relevance to this paper are examined here.[14] Almost all definitions claim that cyberspace is a manmade space or environment, distinct from land, sea, air and outer space. Some definitions emphasise the electromagnetic transfer of information, or the interconnection of systems and networks [57, p. 95]. Others concentrate more on the functionality of cyberspace i.e. the creation, transmission, receival, storage, processing and deletion of data [49, p. 28]. Additionally, some combine these two approaches [58, p. 2]. Yet some take a more holistic view and combine cyberspace with the information sphere or environment [59, pp. 122-123], [53, p. 309]. This approach designates cyberspace as a platform or facilitator for the flow and use of information. Others have tried to separate physical infrastructure, software, rules and processes and information and its users from each other [60, p. 123], [61, p. 5]. The current United States Joint Doctrine defines the 'information environment'

[14] For different concepts see for example [53].

as an aggregate of individual, organisation and system levels and physical, informational and cognitive dimensions [62]. On the civilian side, Martin C. Libicki's division into physical (boxes and wires), syntactic (instructions) and semantic (information) is one of the more influential definitions [63, pp. 12-13]. When it comes to the architecture, cyberspace can be described as a flat, worldwide, interconnected network, without a centre [64, p. 27]. There are also those, who have come to the conclusion that cyberspace is in fact not a separate space or domain, but a 'substrate' underlying all other domains [7, p. 75].

Because this study is interested in the shaping of cyberspace by state actors that carry particular cultural understandings about strategic issues, the following description is used: *cyberspace is an electronic medium through which information is created, transmitted, received, stored, processed and deleted.*[15] The electronic medium highlights the physical aspects as well as the malleable character of cyberspace, and includes a distinction between physical, syntactic and semantic layers. This means that cyberspace can be shaped by intentional actors. Through electronics and the electromagnetic sphere the definition connects cyberspace to the physical world, with territoriality and kinetic effects. The concept of medium allows the separation of cyberspace into different layers that may have different rules. Information gives cyberspace substance, resources, and effects and makes it possible to describe it as a domain, a sphere of human activity[16]. The processing of information (creation etc.) gives cyberspace meaning beyond its borders. The manipulation of information affects human activity. The definition provided here combines structure (medium), substance (information) and processes (creation etc.) and emphasises the technical aspects.[17] It hopefully provides a clearer analytical distinction compared to more holistic and culturally bound concepts of cyberspace or thereof.

[15] The definition is taken from East-West Institute's Critical terminology foundations 2 2014, 17 report [145]. It was a US – Russia bilateral working group that tried to find common definitions for cyberspace terms and policies. Russians do not *officially* use the term 'cyber' but instead use information, which is more holistic [145, pp. 11-12]. This definition is very close to Daniel T. Khuel's [49, p. 28]: "…cyberspace is a global domain within the information environment whose distinct and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."

[16] The term 'sphere' was popularised by Jürgen Habermas. It was originally meant to describe space where thr public opinion is formed. [201]

[17] The cognitive aspect is intentionally left out. Of course, physical, syntactic, and semantic levels provide input into the cognitive level. However, knowledge or cognitive processes are not subject of this paper.

Cyberspace as a domain of human activity has its own characteristics which affect the use of power in and through it. Chouri [61, p. 4] lists instantaneity, geographical transcendence, permeation, fluidity, participation, non-attribution and non-accountability as characteristics of cyberspace. Sheldon [53, p. 288] describes cyberspace as having a low cost of entry, multiple actors, reliance on the electromagnetic spectrum and man-made objects to exists, with constant replication and instantaneity. According to Rattray [65] strategic features of cyberspace are: laws of physics, software logic, mutability, interconnectivity, limited limitlessness (actors have power but it is limited), human resources and know-how. Joseph Nye describes different logics of the levels of cyberspace as "increased returns to scale" and vague limits of jurisdiction on the virtual level and "economic laws of rival resources and increasing marginal costs", and "sovereign jurisdiction and control" on a physical level [58, p. 3]. He also points out that the virtual level provides low cost entry to the physical level and that technology plays a dominant role in the changing character of cyberspace [58, p. 4]. This means that the architecture leads to the diffusion of power and empowers a multitude of actors [58, p. 9]. When discussing cyber deterrence Martin C. Libicki emphasises the role of man-made rules: "The divergence between design and code is a consequence of the complexity of software systems and the potential for human error" [63, p. 18]. He also highlights the problem of attribution, that is, how to link actors in cyberspace to actors in physical world [63, pp. 41-52].

The lists of characteristics presented above have commonalities, but there are also differences. What is more, understandings of cyberspace have changed over time and they overlap. They have gone through visions of self-organising anarchy or a 'the Wild West' to become global commons and are now heading more towards regime or territorial state-centric visions [56, pp. 239-240], [58, p. 15], [66, pp. 61-62], [61, p. 235], [46, pp. 16-18]. From this short summary, the basic characteristics of cyberspace can be deduced as artificial in nature, with a physical base and inherent rules, interconnectivity, mutability, ease of access, a multiplicity of actors, diffusion of power, non-significance of distance and machine speed. This means that, according to leading theorists and theoretical framework adopted in this study, cyberspace is clearly different from other physical domains (land, sea, air and outer space)[18], and can be shaped by intentional and culturally bound states, if they have sufficient resources.

[18] Only land can be shaped by humans, and even then, only on a local level. Additionally, the physical properties of land, do not change.

Furthermore, it can be argued that *cyberspace in its uncontrolled form, is conducive to symmetry in the distribution of power*.

3.4 Definition of cyber power

The reason that the characteristics of cyberspace matter is because power is relational and contextual and cyber power perhaps even more so.[19] In international relations theory there are three or four (depending on view) concepts on power, the so called 'faces of power' [60, pp. 11-14], [67, p. 42]. The first is based on Robert Dahl's formulation of "A getting B to do something B would otherwise not do." (Quoted in [68, p. 4]). This is basically direct power over resources or an effects approach, and sees power or its results as measurable. The second is based on Bacrach's and Barantz's critique of Dahl and states that "…power works more indirectly through both actors being positioned in an institutional setting and the ability of A to influence this setting 'against' B." [68, p. 8]. This approach is interested in agenda-setting and the ability of A to exclude some agendas from political process altogether. The structuralist version of this 'face' is a concept where the positions of A and B order their power relationship without direct intentionality on the part of A [69, p. 450]. The third concept is based on Steven Lukes [70] who was interested in how A can manipulate B's inherent interests, basically changing B's preferences [68, pp. 10-11]. And the fourth, is based on poststructuralists and on Michel Foucault's writings in particular. Here power is seen as productive power, shaping the identities and interests of A and B. [71, pp. 982-984]. It should be noted that all the different 'faces of power' are based on different theoretical premises and are not necessary commensurable.[20]

Theorists of cyber power have had to combine characteristics of cyberspace with different theories about power. One of the most holistic descriptions is Betz and Stevens': "…the variety of powers that circulate in cyberspace and which shape the experiences of those who act in and through cyberspace." [59, p. 44]. This is a product of their attempt to combine all 'faces of power' to one theory and what it gains in brevity it loses in parsimony. Joseph Nye describes it as "…the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. […] …[it] can be used to

[19] This view is taken from Stefano Guzzini's [69, p. 455] analysis of Stephan D. Krasner's [157] and David Baldwin's [158] concept of power. In short, this means that scope, domain, weight, costs and societal norms are dimensions of power.

[20] Barnett & Duvall [67] try to form taxonomy of power based on dimensions direct – indirect, capacity – production. They try to avoid incommensurability by proposing «addition», that is analysing specific issues from different perspectives.

produce preferred outcomes within cyberspace or […] in other domains." [60, p. 8] This is a subject-centric, intentional use of power, compatible with the first and second faces of power, and highlights the fungibility of cyber power i.e. its convertibility and scope.[21] Somewhat similar is Khuel's (2009) version: "…the ability to use cyberspace to create advantages and influence events in all operational environments and across the instruments of power." [49, p. 38] Khuel's definition's value is in that it highlights the possible synergistic effect of cyber power. These formulations seem to suggest that cyber power is compatible with universal definitions ('faces') of power but has its own resources and context which give it a distinct character.

Besides the above presented conceptual formulations, there have been attempts to define cyber power by its resources. Nye, for example, offers infrastructure, education, legal control, markets, budgets, institutions and reputation as power resources of states [60, p. 133]. Brandon Valeriano and Ryan C. Maness propose resource-based concept of power by differentiating between offence (weapons and training), dependence (reliance on the Internet) and defence (resilience, adaptation and protection) capabilities [51, pp. 25-28]. Somewhat similar is a more policy oriented view presented by Chris Demchak: "Cyber power today is defined as the ability of a nation's leaders and institutions facing cybered conflict to keep overall uncertainty across nationally cybered systems down at levels tolerable for their citizens' expectations of normal well-being." [72, p. 128]. From her definition she construes institutions, national mentality and offensive and defensive forces as power resources [72, pp. 130-131]. Considering purely military cyber power Rebecca Slayton has proposed technology, skilled people and well-developed organisations as resources of power [73, p. 86]. It is not surprising that education, technology, regulation and organisation are defined as resources because of the dual physical – non-physical nature of cyberspace. The problem is, that these are more difficult to measure than purely physical capabilities, which have already in themselves proved to be notoriously difficult to measure at least in a military context [74, pp. 14-19], [75, pp. 47-48].

One additional problem is that because there has been no conflict categorised as cyber war, there is no shared understanding of the enabling or strategic role of cyber power, i.e. whether it has independent strategic effect or not.[22] This means that the effect of, at least military, cyber power

[21] See Robert J. Art [159] and David A. Baldwin [160] about the fungibility of power.

[22] Colin Grey [37, p. 20]: "Strategic effect is the impact of strategic performance upon the course of events." This means that the effects of a particular military use of force

is disputed, cf. [76], [77], [51], [7]. Perhaps, a third problem is, whether cyber power should be considered militarily or as a more comprehensive instrument of national or global politics. This might be a normative problem, and as such, beyond the scope of this study. Regarding cyber power's role in the continuum of state relationships, peace and war, Baylis, Wirtz and Gray offer the following helpful definition: "…the ability in peace, crises, and war to exert prompt and sustained influence in and from cyberspace," [30, p. 306]. This definition is important because it takes note of long-term effects and shows that the use of cyber power is not restricted to wartime even if it can be considered to have a military aspect. This means that cyber power might have military effects even if it is utilised in non-military ways.

The definitions above show that cyber power is not confined to cyberspace, it is not separate from other types of power and it can have persistent effects even though its domain is changeable. More clarity is needed if cyber power is to be differentiated from other types of power. This might be achieved through its characteristics. John B. Sheldon describes cyber power as pervasive, complementary and stealthy [53, p. 289]. Stuart H. Starr would not apply principles of war from other domains to cyberspace because cyber power is more diffuse, its speed and scope are different and it is very dependent on technology [78, pp. 56-58]. Elinor C. Sloan takes a more military oriented view and lists unconquerable space, continuous change and adaptability, borderlessness, rapid and potentially wide scale effects and indirectness [44, pp. 89-90]. Joseph Nye offers the extinct monopoly of violence by states, difficulty of attribution, cheap and plentiful resources, low relevance of distance, strength of offense compared to defence, unfeasibility of conquering space or destroying opposing forces and the high fog of war [58, p. 5]. Erik Gartzke and Jon Lindsay note that the effects of cyber power are only temporary and that it is difficult to hoard it, because it is insubstantial and relative and loses its utility when used [46, pp. 345-346]. Libicki [79, p. 35] has declared that there is no forced entry into cyberspace, which means that power is tied to the rules of cyberspace (e.g. if you try to blow your way in, you do not have cyberspace anymore). Maness and Valeriano point out that cyber power can have a spill-over effect into other domains or issue areas [51, pp. 46-47]. There can be unintentional second or third order effects. Other definitions tell us that cyber power has its own physical, logical,

have a direct relationship to policy goals or political consequences [37, p. 296]. According to Hew Strachan [39, pp. 191-192] the enabling effect means that power has only a tactical or operational effect. It does not directly achieve the objectives of war. The concept of enabling is sometimes used interchangeable with 'force multiplier' which means that particular use of force or means enhanced other uses of force [192, p. 60].

organisational and cognitive aspects depending on which level power is used. It may be kinetic or non-kinetic depending on its object [80, pp. 35-36, 182-183]. It seems that cyber power has no agreed definition. There have been great difficulties to measure cyber power or its effects. Further, Western concepts of cyber power have concentrated on the active and offensive use of power. It is necessary to construct a new concept or at least an understanding for analytical purposes for this study.

Because this paper is interested in the military strategic aspects of cyber power and approaches its subject from a neoclassical realist framework, it is natural that the definition of cyber power should be centred on the first and second faces of power. This means that power is seen as a resource, it is used by A to influence B in some context and relationship, but that it is also an effect of the institutional setting. This does not imply agenda-setting, but shaping the space where more direct power is used. Cyber power can have persistent effects and its resources are not necessarily military. This means that space can be shaped and it retains its attributes for a period of time, even outside conflict, and without the participation of military means and resources. The resources may be technological, economic, administrative or political, whichever can be converted to achieve the preferred outcome. In fact, cyber power's resources can be anything if the effect is in cyberspace or transmitted through it. That said, the main resources can be argued to be technological, normative, doctrinal, organisational and professional. Cyber power can be utilised in peace or war time. It can be used to achieve strategic or enabling effects as part of a state's grand or military strategy.[23] So the use of cyber power is planned, intentional, and strategic and it is dependent on the actor's understanding and perceptions of cyberspace and cyber power. In short, *cyber power is an ability that empowers an actor to influence others in or through cyberspace and to shape cyberspace to its advantage according to its preferences*.[24] This is not a universal definition of cyber power, but it is in line with neoclassical realist theory and the concept of strategic culture.

[23] Paul Kennedy [161, p. 5]: "The crux of grand strategy lies therefore in policy, that is, in the capacity of the nation's leaders to bring together all the elements, both military and non-military, for the preservation and enhancement of the nation's long-term (that is, in wartime and peacetime) best interests". Antulio Echevarria [123, p. 42]: "Today, military strategy is typically thought of in terms of four critical variables: ends or objectives (what we want to achieve); ways or courses of action (how we propose to achieve it); means or resources (what we can reasonably make available); and risk (our assessment of the probability of success)." For the evolution of these concepts see Lucas Milevski's "The Evolution of Modern Grand Strategic Thought" [89].

[24] This definition is modified from [162, p. 25].

3.5 Character of cyber power

Before continuing to discuss asymmetry, cyber power's relationship to warfare should be defined. This requires that concepts of military power and strategy are defined. There are no agreed upon definitions of either of them. First, what is meant by power and force respectively has to be clarified. These terms are used sometimes interchangeably in English, which is a cause of no little confusion. In this paper, power in it its simplest form is understood to mean the ability and potential over something. Force means power that has been given (even if only implicitly) direction and/or objective and it is used against something. Force can also refer to military units acting in a coherent manner. Force can be used or utilised when applied for specific effect.[25] In line with these definitions, cyber power might be conceived as a force with violent consequences. Although there is legitimate criticism against defining cyberspace and cyber power in military terms, it does not relinquish us from the fact that cyberspace has become a military domain and as such requires study from a military perspective [81].[26]

3.5.1 On war and warfare

War is a central term for understanding violence in state relations. Carl von Clausewitz's definition of war as "…a continuation of political intercourse, with the addition of other means" (Queted in [37, p. 12]) is a widely accepted but also contested definition of war. Other definitions include for example "an act of violence involving two or more organised groups framed in political terms" [82, p. 218], "[W]ar is a legal concept, a social institution, and is a compound idea that embraces the total relationship between belligerents" [83, p. 6] and "[A]t least 1000 battle-related deaths in one calendar year," [84, p. 537]. There is no clear international legal definition for war, only UN Charter Articles which basically give states permission for self-defence in case of armed attack and prohibits threat or use of force. Furthermore, there is no consensus on

[25] Use of force does not explicitly include clear, political objective. It might be disorganised, mindless violence. Use of force can also be implied, e.g. used to threaten (cf. [163]). Utility implies that force has purpose and it is useful and efficient (function of cost and effectiveness) in the context of pursued objective [164]. This does not mean that force always achieves expected results. Perceived utility might be erroneous if force and object do not correlate, or if outside factors affect the effectiveness of force. [117, pp. 6-8] [89, pp. 146-150]. To utilise force is to use it for achievement of desired objectives.

[26] On militarisation see Dunn Cavealty [165]. Miriam Dunn Cavealty claims that there is tendency to militarise cyber issues.

what constitutes an armed attack [85]. What is apparent from these definitions (or lack thereof) is that war has no single or commonly accepted definition. Terms such as insurgency, conflict (with different qualifications) and war with different additions such as civil war, intrastate war and total war are used in academic and public discourses. This further blurs the understanding of what war is, who is doing what to whom, how and how much – if used without rigour.

For the sake of clarity, this paper follows the core idea of Clausewitz. This is justified because this study is interested in state use of force against other states for political purposes. Clausewitz is not without fault, and has been criticised as being state-centric, and rationalising and universalising war [86], [83, pp. 28-29], [82, p. 220], [87, pp. 57-58], [88, p. 12]. Much of the criticism has been countered over time, or has been adjusted to fit Clausewitz's ideas, and he is still the main authority in strategic studies concerning the concept of war [89, pp. 439-441], [45, pp. 15-17].[27] Clausewitz (and his followers) enshrined the idea of war as a political instrument, and that it is struggle between two opposing sides, and further that it is affected by friction, and that it is of an unchangeable nature (passion, chance and reason) but is 'chameleon' in character. The last premise means that war is an ever changing, historical phenomenon [37, pp. 91-100], [39], [45, pp. 17-20]. One qualification has to be made regarding Clausewitz's theory which is the concept of conflict. He built his theory from the point of view of open hostility between political communities (if 'people's war' is left aside)[28], which means he did not say much about the use of force outside the context of war. Conflict here is defined preliminarily as the use of force below the threshold of open war. It is limited in its means and ends. The concept is needed to understand discussions on cyber power where the difference between cyber war and cyber conflict has claimed important connotations, cf. [51, pp. 31-33].

It should be pointed out that the concept of warfare is closely related but distinct from war. According to the Webster-Merriam dictionary it consists of "military operations between enemies" or "an activity undertaken by a political unit (such as a nation) to weaken or destroy another" [90]. The Cambridge and MacMillan dictionary define it as "the activity of fighting war" [91] [92]. David Jordan et al. define it as "Warfare is thus primarily about the employment of organised violence. It is about fighting." [36, p.

[27] About the concept of warfare: "Warfare is thus primarily about the employment of organised violence. It is about fighting." [36, p. 3]

[28] Clausewitz did write about 'small wars' and 'people's wars' but these were either about irregular troops used along sides regular troops or mobilisation of citizens in defence of country [86, p. 451].

3]. Like war, warfare is an ambivalent concept because it has emigrated from physical violence to cultural, economic and purely political realms. It has acquired qualifiers like information, economic or political warfare. In a way, this problem is inherent in the Clausewitzian idea of the changing character of war and, of course, also in the politicised use of the term.[29]

From the conceptual discussion above, it can be argued that the understanding of war and warfare can change over time. This is apparent in the 'generations of war' writing, where the character of war has been seen changing with the development of human society, mode of production or technology, cf. [93], [94], [95]. These discussions have in part led to concepts such as cyberwar or cyber conflict which try to capture the role of information technology and change of human condition in the context of war, cf. [56].

3.5.2 Cyberwar

In 1993 John Arquilla and David Ronfeldt coined the term 'cyberwar' which: "….refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to "know" itself." [47, p. 30]. Their concept was rooted in the growing role of knowledge in warfare ("…who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries") [47, p. 27] and the need to change the doctrinal and organisational concept of war. During the 1990s cyber war and warfare where subsumed by information warfare on the one hand and network centric warfare (NCW)[30] on the other. The Western world was preoccupied with unconventional and counterinsurgency warfare which also emphasised the information / knowledge side of warfare, with cyber or network operations delegated to a supportive role or tactics. In the beginning of the 2000s the concept of cyber war got a new life. The development of information society emphasised the vulnerability of critical infrastructure and military networks to attacks through the

[29] War and warfare have established meanings in international law which leads to politicised uses of the terms, cf. [166, p. 361].

[30] Network Centric Warfare refers to doctrinal concept developed in the armed forces of United States of America during 1990s. Its main theorists were Arthur K. Cebrowski and John J. Gartska [119].

Internet.[31] This started an intense discussion about the effects of cyber power in warfare: Were they strategic or just enabling?

Already in 1996 the RAND corporation published a report that coined the term ‘strategic information warfare’ (SIW). It speculated that: “the possibility that future adversaries might exploit tools and techniques of the Information Revolution to hold at risk (not to destruction but to large-scale or massive disruption) key national strategic assets, such as initial elements of the national military posture or the national infrastructure sectors,” [96, p. 31]. Later, writers such as Gregory J. Rattray wrote about strategic information warfare which was “…means for a state and non-state actors to achieve objectives through digital attacks on an adversary’s center of gravity,” [57, p. 14]. After 2001 officials and politicians in the United States’ administration started to talk about cyber catastrophes or “Cyber Pearl Harbors” [97, pp. 29-31], [76, pp. 5-6]. There were attempts to understand this new threat by comparing it to ideas about the strategic role of air forces from 1920s or ideas about nuclear forces from 1950-1960s [57], [63]. The cyber threat was joined with terrorism which gave birth to cyber terrorism that could threaten Western civilisation [98, p. 195], [99, pp. 75-76]. Cyber threats have become high priority for states all over the world. Starting from the United States this quickly led to the so called ‘militarisation of cyberspace’ which meant official and public creation of cyber military units, the development of cyber weapons, and writing of state strategies to militarily defend national networks (instead of delegating this to the realm of broader security) and, if need be, to attack a hostile nation’s networks [61, pp. 148-151].

Cyber war ‘hype’ led to a push back from sceptics, who discredited the idea of cyberwar, cyber powers ability to achieve strategic effects by itself, and the ability of cyber weapons to create sustained and kinetic effects (casualties and destruction) on a magnitude compared to conventional weapons [46], [79, pp. 100-101]. Valeriano and Maness summarise this mentality by stating that: “Cyber conflict is reality, but the threat it produces does not meet popular perceptions,” [51, p. 19]. The idea behind using the term conflict lies in the perception that cyberwar has not happened and that cyber weapons, tactics or operations might only have limited effects or that their nature is only exploitative;[32] while at the same

[31] For conceptual and operational histories, cf. [130], [56], [50]. For the concept of ‘information society’ cf. [202]

[32] Frederic Lemieux [167, pp. 1-2] proposes that tactical cyber operations are techniques and practices, cyber operations serve long-term offensive or defensive goals, and strategic cyber operations equal offensive or defensive policies. Thomas Rid and Peter McBurney [139, p. 7] define cyber weapon as: “…weapon as a [computer code] that is

time recognising that cyber operations are an ongoing reality. Chris Demchak and also Brandon Valeriano and Ryan C. Maness even seem to propose that the nature of conflict (widely understood as any competition or struggle between states) has acquired a cyber nature. No conflict can anymore escape the context of information societies where they are waged [72, pp. 122-128], [51, p. 210]. Into this disagreement between 'strategists' and 'enablers' has been added the legal problem of defining cyber warfare in the context of international law. There is no agreed definition on what is to be considered an armed attack in cyberspace, and so no concept of violation of sovereignty in cyberspace, or basis for individual or collective self-defence exist [1][33]. There is an emerging consensus that cyber war will not take place, but cyber warfare as some kind of cyber conflict, cybered warfare, hybrid warfare, political warfare or simply cyber operations in support of other means of state power are possible and, are in fact, already a reality [100], [72], [51].

3.5.3 Use of cyber force

As there have been attempts to fit cyber war in the previous understandings of war, so cyber power has gone through the same process with the ways to use force. Perhaps, because cyber weapons are new and their strategic effects still poorly understood, many of the concepts used to analyse the use of cyber power have come from writers such as Bernard Brodie, Thomas C. Schelling and Herman Kahn and other writers from the Cold War period, cf. [63], [97], [10], [101]. It is argued here that this has led, with slight variance in terminology, to the adoption of a conceptual continuum of concepts of persuasion, deterrence, coercion and brute force as ways to use cyber force.[34]

Persuasion is something like Joseph Nye's 'soft power', meaning agenda framing, persuading, and positive attraction [60, p. 21]. In this view the object of the use of force does not even notice the use of force or accepts

used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things" Joseph Nye [101, p. 48] states that all cyber-attacks to date have been Computer Network Exploitation (CNE) operations, i.e. exfiltration of data, not Computer Network Attacks (CNA) which are designated to disrupt or destroy. Erik J. Gartzke and Jon R. Lindsay [46, p. 347] claim that cyber operations have utility only as reconnaissance or special operations, i.e. as enablers. Betz & Stevens [59, p. 97] propose the concept of 'cyber skirmish' to describe "the constant hum of low-level activity" seen in cyber space instead of cyber war.

[33] Although there have been attempts like Tallinn Manual and Tallinn Manual 2.0.

[34] This taxonomy is based on the activity of the user of force, on the perception of the opponent and on the effects of force.

as legitimate that he/she is being influenced. Deterrence is based on the ability to hurt. It is the threat to use force to make an opponent not to take an action by threat of punishment or by denying his objectives by inflicting unbearable costs. The opponent has to know about the threat. It has to be credible and it has to affect opponent's cost-benefit calculations [102, p. 5], [45, pp. 47-49]. The difference between deterrence and coercion is that coercion is aimed at making or stopping an opponent act in a certain way. It is based on active measures and the power to hurt, and the opponent has to have a choice to comply or not to comply [103, p. 106].[35] Brute force does not include any kind of bargaining or cost benefit calculations on the side of the opponent. Brute force is meant to destroy and kill, to take something or hold something [102, p. 2]. It should be noted that persuasion, deterrence, coercion and brute force are political-strategic level concepts. On a tactical level some concepts loose some of their meaning [102, p. 5].

Both Joseph Nye and Martin C. Libicki have written about persuasion and cyber power. Nye gives it a role in his 'soft power' concept and Libicki writes about the 'friendly conquest of cyberspace'. From their perspective, it can be said that cyber power has an enabling role in persuasion as part of information warfare.[36] Cyber deterrence has been a hotly contested issue. The basic problems with cyber deterrence are attribution, secrecy, proportionality, repetition and escalation. Because of the way the Internet works, it is difficult to establish the identity of an attacker in any meaningful timeframe. This also makes it difficult to tailor deterrence to any particular opponent. Signalling a credible capability to potential opponents is difficult because cyber capabilities are shrouded in secrecy. Proportionality is a problem because there might not be enough information about potential targets, how much the opponent values them, and what kind of second and third order effects might materialise if force is used. Repetition of punishment would be difficult because weapons are one-time-only items. Because there are no rules on cyber warfare and because there might be unexpected collateral damage, escalation is always a problem [63, pp. xiv-xix], [100, pp. 414-417], [104, pp. 128-129], [80, pp. 92-96]. All in all, as Nye writes, deterrence through punishment seems quite difficult in cyberspace. Deterrence by denial, i.e., an effective defence which makes the costs too expensive for potential attackers, might be a better solution [101]. In fact, as time has gone by, and technology and

[35] Thomas C. Shelling [102, p. x] uses the term 'compellence' and positions deterrence and compellence under coercion.

[36] Nye uses also the term 'entanglement' which refers to perception of interdependence and its effect on cost-benefit calculations. Libicki [79, pp. 125-126] refers to this as 'soft conquest' or 'dependency'.

understanding of cyber power have improved, the argument about ‘cyber weapons always getting through’ has changed to careful optimism about the denial aspect of deterrence [73], [105], [106]. Despite the optimism there is still the problem of how to build cyber deterrence so that it does not lead to a ‘security dilemma’, that is, an arms race and unintentional escalation.[37]

The coercive use of cyber power is also a problematic concept and related to the above mentioned strategic – enabling effect disagreement. Martin C. Libicki states that coercive cyber power is restricted because there is no forced entry to cyberspace, its effects are temporary and difficult to measure, and cyber weapons are use-it-or-lose-it items. So even if individual cyberattacks could have the upper hand on defence, they do not necessarily convert to strategic effects [63, pp. xiv-xv]. As Thomas Mahnken states, for cyber weapons to have an effect, they need to be combined with other uses of force [107, pp. 61-62]. This connection to conventional military power and the costliness of effective cyber weapons programme is also a reason why states are still the main players in cyberspace, even though there might be a diffusion of cyber power as Nye claims.[38] Thomas Rid may be the most famous critic of the strategic role of cyber power. He points out that a coercive use has some of the same problems as deterrence. Because of secrecy and difficulties of attribution there may be no clear understanding of who wants who to do what. The effects are often intermediated and delayed. The nucleus of Rid’s criticism is that cyberattacks up until now have been only sabotage, espionage and subversion [76].[39] Of course there have been those, like Kenneth Geers and Richard Clarke and Robert Knake who see offensive and coercive power as having a strategic effect or at least see the offensive aspects as decidedly more powerful than defence [97], [108].

The brute use of cyber power has partly been subsumed by the deterrence / coercion discussion. In a way, the narrative of ‘Cyber Pearl Harbor’ and many of the threats perceived against critical infrastructure is about brute force.[40] Additionally, brute cyber force may be a more technical / tactical

[37] About offence-defence problem and security dilemma see: [168], [169].

[38] Continuing advantages of states, cf. [59, p. 131]; On diffusion, see: [60, pp. 150-151].

[39] Rid has been criticised by, for example, John Stone [77] who claims that Rid confuses force, violence and lethality and states that lethality is not a requisite of act of war.

[40] Cyber-attacks on critical infrastructure may cause death and destruction and beat an opponent to surrender without any bargaining by destroying the foundations of society and government, cf. [57], [170], [108], [135].

level concept.[41] Be that as it may, destroying and killing with cyber power without any element of bargaining has some of the same limitations as coercion. Furthermore, as some have noted, there is no supremacy in cyberspace [63, pp. 141-142]. No one actor can control it in any meaningful way and destruction removes the access to it from both defender and attacker.[42] Taking and holding assets are problematic concepts in a mutable, man-made environment. There is also a fear that the use of brute force on a strategic level could trigger multi-spectrum deterrence i.e. conventional and nuclear counter attack.[43] So, on a strategic level, brute force might be conceivable as an enabling and supporting force, but as the only way to reach political objectives, it could be unreliable and possibly suicidal.

Perhaps, what can be gained from the discussion above is that cyber power in all its forms differs from conventional military power in its character and utility. Furthermore, the way actors perceive cyber power may affect their behavior. There might be different solutions and uses based on the strategic culture of the decision makers.

3.5.4 Military strategy

The use of force and our concept of cyber power require intentionality. This issue is captured by the term strategy. Strategy as a term has lost its connection to military issues and has become a synonym for ‘a plan’ [39, pp. 249-252]. Nowadays it is necessary to add ‘military’ in front of strategy to make it clear that what is meant by it is: “…the use that is made of force and the threat of force for the ends of policy,” [37, p. 17]. This is, of course, only one way to define military strategy. What should also be kept in mind is that there are at least “…two opposing wills using force to resolve their dispute,” [109]. Strategy is “the art of creating power” [110, p. xii] and “a plan of action designed in order to achieve some end,” [111, p. 14]. It is also a process to identify the character of future war, prepare for it and manage it [112, p. 36], [37, p. 24], [39, p. 118]. According to one influential description strategy is “concerned with ways to employ means to achieve ends,” [110, p. xi]. Hedley Bull echoes this by stating:

[41] Adam Liff [100, p. 405] sees it as a measure to reduce an adversary’s abilities or to frame other actors.

[42] This view contradicts current Western and Russian military doctrines which emphasise the importance of gaining ‘information superiority.’ [203] [204]

[43] See Maness & Valeriano [51] on this and their criticism about it. According to Dmitry Adamsky [26] this kind of approach is built into Russian strategic thinking. Cimbala [171] gives a warning on accidental nuclear war as a product of information warfare.

"[military strategy], it is the art or science of exploiting military force so as to attain given objects of policy," [113, p. 593]. Military strategy can even be considered a culture bound vision of the use of force, although that would bring it very close to the definition of doctrine [37, pp. 141-150].[44] Strategy is related hierarchically to concepts of operational art and grand strategy. Operational art is usually defined as the use of a campaign for the objectives of war and grand strategy as the coordination of all of a nation's assets to pursue policy objective.[45] It should, yet again be pointed out, that strategy is a cultural concept, and different nations and militaries have different notions of strategy.[46]

From an analytical perspective it can be summarised that military strategy has at least five aspects. First of all, it can be a theory about the conduct of war (military theory). Secondly, it can be a concept about national security objectives and character of war (i.e. national security concept). Thirdly, it can be a concrete plan of how to fight a war and what forces to develop for it (strategic level operational planning). Fourthly, it can be a process of analysing the environment and formulating plans. Fifthly, it can be the conduct of war on the highest level (theatre level warfare). These aspects are based on the notion that military strategy is subordinate to policy. Strategy gets its objectives from policy and transforms them to military ends achievable by military and non-military means.[47]

Cyber strategy has been used mainly in the sense of planning and policy concepts. Almost all countries of the world have some kind of cyber security strategy that defines threats and opportunities, responses, responsibilities and resources and some kind of a vision.[48] These strategies are not military strategies, but whole-of-government policy concepts. They are also mainly written around the concept of cyber security, which is a contested concept, and based on risk analysis. They do not differentiate between malicious and unintentional motivations [114]. This official or everyday use of the term cyber strategy is too narrow for the purposes of this paper. That is why Lawrence Freedman's definition of strategy is used: "Strategy is the art of creating power," [110, p. xii]. Behind this short definition is the view that there are political ends which are achieved by using particular ways utilising particular means. However, Lawrence

[44] On doctrines: [172].

[45] These concepts are naturally historical and contested see: [89].

[46] According to Timothy Thomas [3, pp. 468, 476] China and Russia, for example, have their own concepts of military strategy.

[47] Colin Gray [37] is perhaps the most prominent scholar arguing for the need to subordinate strategy to policy.

[48] See CCD COE web page for the list of cyber strategies [24].

disputes that this is just a rational, materialistic plan. The unpredictability of human affairs challenge desired ends and may change calculations altogether. Furthermore, strategy consists of active interaction with bargaining, negotiation, threats, pressure and physical effects [110, pp. xi-xii].[49] And what is most important, interests that define ends are socially construed needs [115, pp. 275-276].

If power is understood as an ability to affect our surroundings and other actors, to create an effect, then this is in line with this paper's theoretical framework and concept of power. It is not just a plan or direct use of force. It allows for multiple resources, ways and means to create effects. This concept is also in line with Joseph Nye's understanding of power resources which are converted in some context and relationship, in different ways (modalities), to power [60, pp. 40-41]. This formulation goes beyond the purely military use of force, and permits concentration on non-kinetic and non-military means to use cyber power for military ends during peace and wartime and between them. If Edward Luttwak's observation of 'paradoxical logic of strategy' - is never acted on a passive opponent and there is no universal winning strategy - and that this concept is added to Freedman's and Nye's ideas, it is clear that strategies evolve and may create unforeseen consequences. To sum it up, if the definition of cyber power was that it 'is an ability that empowers an actor to influence others in or through cyberspace and to shape cyberspace to its advantage according to its preferences', a strategy is one component of that ability when considering the use of military and non-military force in the context of cyberspace. Next, this paper moves on to examine asymmetry, its conceptual history and relationship to cyber power.

4 Asymmetry

The concept of asymmetry is not solely the property of international relations or strategic studies. There might be grounds to study asymmetrical cyber issues from economic or purely technological points of view. But because this paper is interested in the use of cyber power in military contexts, the conceptual history is based on how asymmetry has been understood in the context of the use of force.

[49] Here Freedman is very close to André Beaufre's definition: "the art of the dialectic of two opposing wills using force to resolve their dispute." (Quoted in [37, p. 18])

4.1 A short history of asymmetry

Every conflict has asymmetric characteristics [39, p. 22]. There are always vulnerabilities and differences in power, and strategy is based on the exploitation of an opponent's weaknesses [60, p. 34], [110, p. 227], [39, p. 22], [116, p. 78], [117, p. 6]. Nevertheless, the concept of 'asymmetric warfare' has appeared and there are universal features of how asymmetry is defined in military thinking. Generally, these features relate to unequal military resources and the use of unconventional methods to exploit the vulnerabilities of the adversary.

According to Lawrence Freedman, the idea of asymmetric conflict made its appearance in Western military thinking in the 1970s [110, p. 52]. It was not until 1990s that asymmetry reached the level of doctrines and strategies first as an advantage but then quickly changing to vulnerability as the United States began to confront insurgent forces in international operations [118, pp. 3-4]. During the 1990s and 2000s, thinking on asymmetric warfare intertwined with discourses of revolution on military affairs (RMA), network centric warfare (NCW) and new generation warfare (NGW) [48], [119], [120], [94], [121]. These discourses were fueled by a perceived change in the character of war, which was attributed to declining state power, the rise of non-state actors, the growth of information society and cultural factors [87], [122], [82]. Basically, asymmetric warfare came to be defined as something carried out by non-state actors against military superpowers or coalitions that relied on high-tech conventional capabilities and methods and was restrained by fear of casualties and collateral damage [95], [94], [117].

There were differences of opinion inside this, basically Western view. During the 1990-2000s, there was an argument between the so called 4GW (Forth Generation Warfare) thinkers and official NCW proponents. Both tried to legitimise their views on restructuring and re-tasking modern military forces [74], [95], [93], [123]. The idea that war was somehow changing with the development of the information society and that networked non-state actors were becoming the principal adversaries clashed with the idea of the triumph of Western military technology and continuing relevance of conventional military power maintained for intrastate war. There was also a conflict between the importance of culture and information versus technology. In the writings of the 4GW thinkers, asymmetry was not so much a result of power differences so much as differences of will, objectives, organisation and norms regulating behavior.[50]

Later on, the evolution of the U.S. Joint Doctrines introduced ideas about full-spectrum dominance and cross-domain deterrence which also affected ideas about asymmetry [46], [123]. What these concepts meant from asymmetrical point of view was that there could be fatal vulnerabilities in any of the domains of warfare (land, sea, air, space and cyber) which could be used by an adversary to bypass strengths. Increasingly towards the end of the 2000s military minds in the West (and China and Russia) were worried about information as a vulnerability and its use as a weapon. It was seen to be able to deter and coerce, and to win wars without firing a shot by breaking the will of the opponent, and to paralyse opponent's military forces. In all of these considerations cyberspace, as an underlying infrastructure of information, had a prominent role.[51]

The latest incarnation of asymmetry has been the appearance of so-called hybrid warfare. Hybrid warfare in fact has its roots in the same 4GW discussion mentioned above but was raised to the level of nation states by illegal annexation of Crimea by the Russian Federation.[52] In the context of hybrid warfare or operations, asymmetry is not seen as much as a type of conflict or difference in power, but as means and methods.[53] Creativity, flexibility, indirectness, adjustability and initiative are seen as building blocks of asymmetry. Hybrid war is in a curious way a concept shared by both the West and the Russians. The difference is, who is waging it against whom [124]. The latest concept to (re)apper has been political warfare.[54] It has its roots in the Cold War and is formulated by George Kennan as "…employment of all means at a nation's command, short of war, to achieve national objectives. Such operations are both overt and covert." [125]. Because of the current international the political situation, a more traditional approach to asymmetry has also reappeared. It compares specific, measurable, with capabilities to find asymmetry (for example missile defence versus MIRVs) and is reminiscent of Cold War era

[50] On this discussion, cf. [95], [94], [173], [93], [110, pp. 225-227].

[51] About these visions see: [174], [129], [63], [97], [147], [5], [50].

[52] Examples of this discussion, see: [175], [176], [146].

[53] According to Frank Hoffman's [175] concept of hybrid warfare, asymmetry is not seen so much as a type of conflict or difference in power, but as means and methods. Currently there is a debate going on as to whether, instead of warfare, we should consider hybrid operations as part of political warfare or as some type of NGW [198], [199], [200].

[54] See for example: [146].

calculations.[55] These asymmetries could be based on quantitative or qualitative assessments. Considering how asymmetry has 'come back from the cold' i.e. returned to the strategic, state to state level, cyberspace has a natural place in 'hybrid' or 'political' warfare as it provides an avenue for messaging, pressuring, and limited their use of force under the state of war as a part of normal political competition, and, if need be, as a part of escalation.

4.2 Different understandings of conventional asymmetry

There is no coherent theory or widely accepted concept of asymmetry of military power in international relations or strategic studies, but still there is sufficient uniformity that it is possible to speak about certain phenomenon. To find out what characteristics have been connected to asymmetry some of the most prominent definitions in the literature are presented below.

In 1998 Lawrence Freedman separated three kinds of asymmetry: power, means and interests. The first was related to the objective balance of military power between opponents, the second to means used by one of the belligerents which somehow gave it an advantage, and the third to difference of interests, which would give the other an advantage, because it had greater will or led the other to fight the wrong kind of war. The last would give rise to asymmetric strategies which Freedman described as aiming to inflict pain instead of trying for victory, playing for time and targeting the values of opponent. It seems that Freedman also considered NBC weapons as a source of asymmetry [110].

Metz and Johnson wrote in 2001 that "[S]trategic asymmetry is the use of some sort of difference to gain an advantage over an adversary," [118, p. 1]. They studied the doctrines and strategies of the United States and called for a deeper understanding of asymmetry than just "not fighting fair". They proposed the following definition:

> "In the realm of military affairs and national security, asymmetry is acting, organizing, and thinking differently than opponents in order to maximize one's own advantages, exploit an opponent's weaknesses, attain the initiative, or gain greater freedom of action. It can be political-strategic, military-strategic, operational, or a combination of

[55] This is closely related to offense – defence theory [74]. Evidence of this thinking can be found in [177], [178]; And on the Russian side [124].

> these. It can entail different methods, technologies, values, organizations, time perspectives, or some combination of these. It can be short-term or long-term. It can be deliberate or by default. It can be discrete or pursued in conjunction with symmetric approaches. It can have both psychological and physical dimensions." [118, pp. 5-6]

Although Metz's and Johnson's definition might be all-encompassing, it points to many interesting elements. First is the idea of thinking differently, which means creativity. Second is the difference between using weakness or creating an advantage, in that asymmetry is not passive. Third comes using symmetric and asymmetric approaches together, which separates asymmetry from the character of conflict. It is clear that for Metz and Johnson asymmetry was a result of a particular kind of behavior, not the character of a particular kind of conflict.

A little later than Metz and Johnson, Morgan Forrest et al. proposed the following definition of asymmetry when studying escalation: "An asymmetric strength or weakness is simply a quality of one adversary that the other lacks in kind to a substantial degree. An asymmetric attack is one that exploits such a mismatch in capabilities or some undefended weakness, regardless of the nature of the weapon or tactic employed," [126, p. xv]. What is interesting in this formulation is the qualifier: "to a substantial degree". This implies that asymmetry could be somehow measured and that asymmetry relates to capacities or characteristics of belligerents.

This kind of approach was taken by Ivan Arreguin-Toft who studied why weak actors win wars against stronger ones. He based his analysis on quantitate power and argued that strong powers choose the wrong strategies, which is perhaps connected to the socialisation of states. Wrong strategies lead to longer conflicts which lead to domestic dissatisfaction in stronger states. Although Arreguin-Toft did not directly study asymmetry, his study points out that asymmetry might not stem from vulnerabilities, power differences or even methods, but different understandings of war and different force structures based on those understandings, and also from domestic attributes of one of the belligerents [127]. Stephen Biddle, like Arreguin-Toft, studied military power from a quantitative perspective and although his understanding of military power is very much capability based, he comes to the conclusion that, in fact, victory and defeat are dependent on doctrine – force employment [74].[56] There are seeds of

[56] Bert Chapman [172, p. 2] defines doctrine as providing: "…a coherent and consistent framework of concepts, tenets, and principles that are applicable in planning and

asymmetry in how forces are organised, trained and used in combat. Biddle's study considers tactical and operational levels, but according to Barry Posen, doctrine is nevertheless something that interacts with strategic situational assessments. Doctrines have their own effect on how states perceive international system and prepare for war [128, pp. 15-16].

It is interesting to note that not all of the 4GW writers used the concept of asymmetric warfare. For example, Thomas X. Hammes did not use it in his book "The Sling and the Stone" [94]. Perhaps this is because they were describing a new kind of warfare, not an anomaly. What their critics have nevertheless pointed out, is their fixation on non-state, networked actors [95, p. 242]. There is then a tendency to see asymmetry growing out of the character of the actors – i.e. states versus non-states. States are seen as unable to use their whole power resources against non-state actors mainly because of collateral damage and inability to convert power to strategic effect (usually 'winning the hearts and minds' of the population of area of operations).

Even if some of the 4GW writers did not specifically use the term asymmetric warfare, it did appear in official national and military documents, which spurred further writing among scholars.[57] It started to appear in text books under the guise of 'irregular warfare' where it was defined in one instance as: "the use of violence by sub-state actors or groups within states for political purposes of achieving power, control, and legitimacy, using unorthodox or unconventional approaches to warfare owing to a fundamental weakness in resources or capabilities," [36, p. 232], [44, pp. 65-66]. These descriptions were very much in line with what Lawrence Freedman had already stated in 1998. Here an argument can be made that asymmetry, even if implied, was very much understood in the context of its time, the so called 'War on Terror', which affected the United States and its allies. This view was shared by such luminaries as Lawrence Freedman and Colin Gray who explicitly connected asymmetric warfare to insurgency warfare [129, p. 50], [83, p. 245]. Freedman brought up such components of asymmetry as geography, better ability to sustain pain (cost), patience, disregard for casualties and control of narrative. The last one is interesting because it connects information to asymmetry. This was not 'information superiority' as understood in the context of network centric warfare, but control of opinion and truth.

conducting operations, and that these doctrinal attributes are intended to assist in developing and executing operational plans."

[57] This was apparent, for example, in the establishment of academic journals like "Dynamics of Asymmetric Conflict" in 2008 [179]; Cf. Ivan Arreguín-Toft on development of theories of asymmetry in 2000s [131].

Beginning from 1990s the NCW produced a different version of asymmetry in the context of information warfare (IW)[58]. NCW was in some ways contrary to 4GW, because of its emphasis on technology and information. It was conceptualised by Arthur Cebrowski and John Garstka and it had a definite impact on the United States' and its allies' militaries. According to Paul Mitchell (2006) the idea of the NCW was to share information inside a network, which would lead to faster decision making and efficiency. Although Mitchell is a critic of the NCW concept, he seems to accept its basic premises, which is that information superiority can be achieved by protecting one's own information assets and denying the opponent his/hers. Although Mitchell did not discuss asymmetry it was clearly present in the NCW thinking. It is the idea that by controlling information and processes connected to it, a belligerent can get inside opponents decision making cycles, destabilise him/her and destroy or bend him/her to his/her will [130].

After 2010 a more critical and varied view approach to asymmetric warfare appeared. In 2011 Jesse Chace, for example, criticised the doctrinalisation of asymmetric warfare and stated that the core of asymmetry was in imagination [121]. In 2012 Arreguin-Toft brought up his previous study about weak actors winning wars and linked it explicitly to asymmetric conflict. He mainly pointed out that power differences may not be the only source of asymmetry as the United Stated armed forces had codified in its doctrines [131]. In 2013 Lawrence Freedman in his magnum opus Strategy – a History heavily criticised both the 4GW and more technologically oriented thinking. This was, of course, easy to do after the United States had become mired in Iraq and Afghanistan for ten years. He basically restated his 1998 views on asymmetric warfare. In his critique Freedman sheds light upon one important aspect of asymmetry: it seems to be quite hard to neutralise an asymmetric advantage once it has been acquired [110, pp. 220-236]. In the same vein Hew Strachan declared in his book "The Direction of War" that there was nothing new in asymmetric warfare. His perspective was historical and connected to insurgencies, and was critical of the concept of 'new wars.' What Strachan manages to do quite credibly is to show that asymmetric warfare understood as only 'small wars' or 'insurgencies' is not a plausible notion, asymmetry is part of all kinds of warfare [39, pp. 21-22].

[58] IW is used here to denoted particular 'proto-doctrine' developed in US DoD [130, p. 31].

Lucas Milevski (2014) tried to save the concept of strategy from 4GW thinking and cultural bias (euro centricity) by stating that "strategy may be interpreted as the generation and exploitation of asymmetry for the purposes of war," [116, p. 79]. He separated conventional asymmetry from unconventional asymmetry. The first was related to a conflict between equal actors and the second to insurgency warfare, where the power relationship was unequal [116, pp. 80-81]. When writing about military theory Angström and Widen characterised asymmetry as distribution of force, and differences in quality and type of organisation, as well as means and norms. They criticised the tendency to divide wars according to the means used. Means could be used on tactical level or for strategic effect – they do not characterise war in themselves. Throughout their book Angström and Widen make it clear that there are two inner tensions inside military theory: rationalism versus constructivism, and explaining versus normative approach [45]. This means that constructing an objective and universal concept of asymmetry in military affairs may be futile.

The growth of interest in A2/AD (anti-access/area denial) capabilities in the United States armed forces, first because of China's actions in the East- and South-China Sea, and after 2014, Russia's actions in the Baltic Sea and Black Sea areas, brought geography into an asymmetric context.[59] This was part of the latest doctrinal evolution step in the United States joint doctrine and demonstrates how the understanding of asymmetry is connected to wider doctrinal understanding of war. The asymmetry in A2/AD is the ability of one of the belligerents to deny the freedom of movement on a particular area with the use of combined military capabilities [123], [132], [133]. The term asymmetry is not (yet) widely used in Western writings in the context of A2/AD which might be because asymmetry is associated so strongly with insurgent warfare. Nevertheless, asymmetry as a form of controlling and closing information space is implicitly present in the case of NCW.

[59] Cf. Lasconjarias & Marrone [195]; [148]; Sam J. Tangredi [180] on the concept of A2/AD: " In short, A2 (anti-access) is a strategy in which combat operations are but one part. In contrast, AD (area denial) represents tactics that can be used to achieve A2 objectives in a military campaign, but are largely indistinguishable from "standard" land warfare or sea denial operations. AD can support an A2 strategy, or can support another strategy. "If an opposing force needs to apply area denial (AD) tactics in a combat situation--particularly on land--then we have already won the A2 phase of a protracted conflict. […]An anti-access strategy is a plan for keeping a strategically-superior military away from one's region. It is intended to either deter interference by an outside power while achieving a regional military conquest, or if deterrence fails, achieve a quick victory while avoiding a force-on-force contest."

Alongside the A2/AD discussion, unconventional warfare is also going through a slight evolution. One example is Joseph Votel et al. [134] who write about ‘Gray Zone’ operations in the context of political warfare. Their ideas are connected to the hybrid war discourse and they map out a new role for special operations forces (SOF) in future conflicts between open diplomacy and open warfare. Interestingly, they define victory in such a context as: “…retaining decision space, maximizing desirable strategic options, or simply denying an adversary a decisive positional advantage,” [134, p. 108]. With their focus on SOF and ‘Gray Zones’, Votel et al. disconnect asymmetry from non-state actors and open war or conflict. The search for a strategic advantage directly connects to the shaping phase of operations and elevates it to a possible decisive part of conflict.[60] James J. Wirtz basically shares the ideas presented by Votel et al. but offers a more strategic perspective on ‘Gray Zones.’ He presents three traditional ‘short-of war’ strategies (fait accompli, proxy warfare and “salami tactics”) that states can use when they want to avoid direct war and argues that the change of international system has made these strategies easier to use. ‘Short-of-war’ strategies attack an opponent’s strategies and their inherent weaknesses, relying on a target’s inability or unwillingness to react, and can therefore be considered asymmetric in character [135].[61]

The concept of asymmetry is contextual and has changed over time, but there is still enough consistency that it can be argued to be a meaningful concept inside an international relations and strategic studies framework. It is also a cultural concept which means that it can be expected that, for example, the Russians and Chinese will understand it more or less differently. This is in fact one of this paper’s main arguments. The fixation on non-state actors and insurgencies has up until recently hindered our understanding of how asymmetry has been understood in different cultural contexts. What is more, the implicit perspective that asymmetry is something an adversary does to us (Western militaries) has blocked us from seeing asymmetry ‘from the other side.’ Maybe, asymmetry is not what you are, what you have, or what methods you use. Perhaps, it is not even about the rules of the game. It may be about how you play the game (or even win) before it has even started.

[60] Cf. Phases of operation in US armed forces JP 3-0 [181].

[61] Van Jackson proses an almost identical definition but warns against conflating conflict types with tactics. ‘Gray zone’ should be understood as description of strategic competition. [196].

4.3 Ex-ante asymmetric cyber warfare

Cyber power or warfare have not been untouched by the larger discussion on asymmetry in a military context. Non-state actors have been at the forefront of security studies concerning cyberspace. The discourse on cyber terrorism has been ongoing since the 1990s and has had an effect on national cyber security strategies at least in the USA and Europe [50], [18], [136]. Hackers and criminals have also been seen as a serious security threat to the information society [137], [136]. These threats are by their nature also asymmetric. Furthermore, the concept of critical infrastructure, which is an essential part of understanding information society and cyber warfare, is in its nature asymmetric. It is based on the perceived critical vulnerability of modern, advanced states to attacks using low-cost means by state and non-state actors [138]. Narratives on 'Cyber Pearl Harbor' or similar catastrophes are based on the idea that malevolent actors can inflict disproportionate damage and nation states are unable to deter or punish the perpetrators. The whole notion of cyber warfare has been described as unconventional and asymmetric by Kenneth Geers [97].[62]

As this paper has already noted, discussions on cyberspace and cyber power have a tendency to see cyberspace as inherently asymmetric in the sense that it allows non-state actors to use low-cost means against stronger opponents (i.e. diffusion of power). There are, of course, those who dispute this view by stating that even if states are unable to deter all attacks they have the resources to retaliate which could raise the potential costs of aggression. Given time, attribution is doable and punishment can be delivered by other means than cyber [63], [46], [107, pp. 61-62]. As David Betz and Tim Stevens have noted [59, p. 93], there is also an asymmetry between open and closed networks, so asymmetry is not only the attribute of cyberspace as a whole but also exists inside it. Views presented above, of course, challenge the notion of a 'borderless' cyberspace where power distribution naturally strives toward symmetry. This contradiction stems from the view that non-state actors themselves are somehow 'asymmetric.'

According to Adam Liff one of the basic premises of cyber warfare is the asymmetric characteristic of cyber weapons. They are cheap and effective, and readily available. Liff criticises the way in which these attributes have been inflated to mean that the offensive rules over the defensive and that this will lead to war [100]. The character of cyber weapons has also been

[62] Cf. Similar notions [61, pp. 223-224], [58, p. 5].

questioned by Thomas Rid and Peter Burney who state that the so called cyber weapons seen this far have, in fact, not been weapons, but exploitation and intelligence gathering tools. Real weapons require state level resources and are unique. Rid and Burney use this as a proof that the widely held notion of offensive superiority is false [139]. In a different article Rid writes with Buchanan that the attribution problem is also over-inflated. They divide attribution to tactical (how), operative (what) and strategic (who & why) levels, and argue that by combining these, attribution is achievable – in fact, this is more and more so as technology advances [106]. Writings by Liff and others show that the offense – defence asymmetry of cyberspace, mainly based on superiority of offensive and problems of attribution, is being debated.[63] It also shows that the asymmetry discussion has been centred on means and actors.

As with kinetic versions of asymmetry, thinking about cyber asymmetries has been changing during the 2010s. There are at least two reasons behind this: the rise of the concepts of resilience and A2/AD. The first is connected to a larger change in the understanding of state and civil society security. Cyber resilience is still an evolving concept, but it can be defined as, for example, "the ability to prepare for, adapt to, withstand, and rapidly recover from disruptions…" [140]. The idea is to promote whole-of-government approach to cyber security and at the same time relinquish the idea of perfect defence or even deterrence. Cyberattacks happen all the time, some will get through and the idea is to minimise the effects (risk) and maximise the costs of the attacker. So, resilience can be described as an attempt to even out the perceived advantage of an offensive with deterrence by denial. Alison Lawlor Russell brings the A2/AD concept into a cyber context in her book Cyber Blockades (2014). She defines 'cyber A2/AD' as: "Deliberate actions to deny a state access to cyberspace and/or diminish its capacity to operate freely therein," [141, p. 154]. She argues that because of the physical layer of cyberspace, it is vulnerable to destruction and disruption, but this requires large scale use of force on different levels (physical and syntactic). What the A2/AD and resilience concepts demonstrate, is that there is a growing tendency to see cyberspace in perhaps more traditional, state centric, territorial ways. This brings forth questions regarding environment, position, movement, borders, avenues etc. when discussing about asymmetry.

[63] This debate takes some of its premises from offense – defence theory which is further proof of the notion that cold war era concepts are being adapted for the information age. See Robert Jervis [168, pp. 187-190] on offence – defence balance and Charles L. Glaser [182, pp. 194-199] on its criticism.

One of the latest and most interesting definitions of asymmetry in cyberspace is offered by Oehmen et al. [142] [143]. They describe asymmetry as "…a disproportionate, exploitable imbalance between actors related to, but not limited to, resources, level of effort, risk, or consequences in attack." They formulate their definition to help them study asymmetry from the point of view of enhancing cyber resilience and defence. Theirs is not a behavioral concept or attached to certain kind of actors. It does not include exact means. It describes a positional relation between actors which, hopefully, can be measured. What their definition lacks is context. It leaves open the question, whether asymmetry can be compared in one relationship to another. Oehmen et al., like Milevski, divided asymmetry into numerical and capacity differences. Both are relational, but the first one is commensurate, whereas the second one is a fundamental, disproportionate, multiplying advantage. What is interesting from the point of view of this study, is that Oehmen et al. connect capacity to the ability to influence terrain and to disproportionately favour the defender. This of course, is in line with our definition of cyber power.

Although Oehmen et al. and others opened a new view on asymmetry as the shaping of cyberspace, their view is still one sided. It suffers from a kind of (Western) cultural bias, an artificial dichotomy between offense and defence, and the basic flaw of forgetting the 'dialectic of force'. In the next chapter the different understandings of asymmetry brought forth above will be categorised and then a new one will be proposed for the study of shaping cyberspace by state actors to gain both defensive and offensive advantage and to gain control over opponent(s) even before open conflict or war.

5 Structural cyber asymmetry

Until recently, the traditional concept of asymmetry has been tied to a notion of weaker, possibly non-attributable, non-state actors using unconventional means as the basis for asymmetric warfare. This paper argues that, this is a far too limited perception of asymmetry in cyberspace. The reason is, firstly, that there is more to asymmetry than non-state actors and unconventional means. Secondly, cyberspace is artificial and can be shaped according to security needs of states. Thirdly, some states are willing to depart from the idea of global commons towards nationally controlled closed networks by delimiting networks, controlling their infrastructure, and restricting the flow of information. Fourthly, closed networks provide both defensive and offensive advantages. From one point of view, the aspiration of some states (i.e. Russia and China) to build 'digital sovereignty' can be seen as a legitimate effort to limit and contain asymmetry rising from dispersion of power and perceived vulnerabilities. From a different point of view, this process hides behind it the building of a different kind of asymmetry.

This paper argues that this process creates a new kind of asymmetry, which is based on the shaping of space, and names this 'structural cyber asymmetry'. By concentrating on traditional asymmetrical threats in cyberspace, and projects to counter them, a deliberate strategy project by Russia and some other states to create asymmetry in cyberspace by digitally and physically controlling certain national and territorial parts of the Internet is missed. Their short-term goals are military and economical; the long-term goals are directed against the so-called Western world order.

As has been argued previously by Kukkola et al. [8] [9] asymmetry in cyberspace is created by shaping the cyberspace, i.e. the process of closing national networks creates 'cyber asymmetry'. Here this concept is refined and developed further by examining sources of asymmetry, by concentrating on space (i.e. cyberspace as digital territory and as a battlefield)[64] and by placing asymmetry in the context of cyber power defined earlier. Then the effects of asymmetry, its sources and context are considered and categories are formed for the study of real life phenomena.

Based on Chapter Four of this paper and previous studies [9] asymmetry in a military context seems to have at least five different meanings. The first is based on resource differences and is usually attached to peer competitors. This is usually understood in terms of power differences between weak and strong states, and states and non-state actors. Second is relational and based on fundamental differences in capacities. These can be understood as capabilities, means, information[65], doctrinal and organisational differences, norms and culture. These asymmetries are contextual and relative to the relationship under consideration. They are fundamental strengths and vulnerabilities. Third is also relational, but based more on character of conflict and belligerents' perception of it. It consists of will, interests and objectives. These are more insubstantial but

[64] The term 'digital territory' is used here to separate cyber space from outer space (i.e. rest of the universe outside Earth's atmosphere) and more abstract concepts of space. Also, 'digital territory' points to objects, distances and quality and quantity of connections between objects. It is the infrastructure of cyber space that can be mapped out and analysed for determining asymmetries. It gives structure to cyber space. It is the 'level' upon which cyber battles are fought.

[65] Information permeates cyberspace as a construct, process and substance. Thus, it could be considered for all meanings of asymmetry presented here. For clarity's sake, it is placed under capacities in this study.

affect cost-benefit calculations. The fourth meaning is related to space (i.e. digital territory). It is structural in the sense that it is an attribute of context (in this case a battlefield) and affects all belligerents based on their position. It enables or restricts actors' ability to observe their surroundings, project power and protect their assets. The fifth is time. Time can be understood as a property of an actor in the sense that one could have a different sense of time. It can be characterised as resource, because one actor could have more time to achieve its objectives, or need less time than its opponents. Time is also connected to space. Distance translates to time. In fact, time and space are so interconnected in military issues that their separation is almost futile. The sixth aspect is imagination. This is, in a way, the ultimate enabler and can create asymmetry based on pure creativity.

Based on the fourth meaning of asymmetry presented above, the structure of cyberspace is a possible source of asymmetry. The structure can be analysed as 'digital territory' consisting of objects, routes and distance between objects, and borders between subspaces. From the previous discussion and definitions (ch. 3 & 4), the following arguments are deduced: In cyberspace objects consist of infrastructure, software and processes, and information (stored or 'flowing'). Routes can be physical or logical. Physical distance between objects has little consequence. Digital distance is more important. This can be defined as a function of routing (hops, steps etc.). At the moment, national or territorial borders have little effect on cyberspace, but this might change. Firewalls, filtering, routing, subnetworks and AAA –policies (authentication, authorisation, and accounting) are building blocks for borders, and in a military sense, frontlines. Borders are created inside cyberspace by creating subnetworks or air-gapped networks, or by traffic monitoring and filtering.

Cyberspace as 'digital territory' differs depending on the level of analysis. On the physical level, it consists of electromagnetic radiation, cables, satellite links, radio connections, routers and switches. At the syntactic level it consists of networks that are composed of subnetworks, protocols, software, encryption, routes, bandwidth, hosts, services etc. On the semantic level it consists of information. Because cyberspace is partly a non-physical and manmade environment, norms, rules and governance are an inherent part of it. They are not laws of nature, but they are ever-changing and open to manipulation. Cyberspace is mutable and it operates at machine speed. For the above-mentioned reasons, cyberspace is not the same for all or everywhere or every time, and this gives rise to asymmetry.

Because time and space are interconnected, time has to be noted, although, in this paper, space is the independent variable in the relationship. The shaping of space affects time as a resource. Time is important because it has central part in decision-making and in achieving initiative and surprise. In Western military thinking John Boyd's OODA Loop (Observe-Orient-Decide-Act) has been used to describe a process whereby faster decision making can give belligerents an advantage over their opponent, forcing the opponent into a reactive state and perhaps into total collapse.[66] The OODA Loop is a simplified description of decision making and it can be argued that it does not capture processes very well in complex or novel situations, and gives undue value to the speed of decision making. Speed of course is not everything; lack of time, bad intelligence, biases or hasty actions can lead to suboptimal decisions. [67] Nevertheless, there is an important temporal aspect in decision making. An advantage in the speed of decision making might give a belligerent the ability to control the opponent by forcing him/her to react in certain ways by denying freedom of action or by threatening important assets. Traditional military thinking also holds that time might be traded for space and vice versa [144, pp. 151-156].

The definition of cyber power proposed earlier was that it "is an ability that empowers an actor to influence others in or through cyberspace and to shape cyberspace to its advantage according to its preferences." To power was added strategy as an integral component of that ability. Taking note of what has been stated about asymmetry in general and cyberspace's digital nature in particular, a concept of 'structural cyber asymmetry' is offered. It is a relational and structural (but not structuralist)[68] concept and based on the understanding that cyberspace can be shaped to the advantage of a state. Although structural asymmetry is connected to the resources of a nation, asymmetry is not a direct result of utilising those resources, but is intermediated by the attributes of cyberspace. Structural asymmetry is not then a resource or capacity of actor, but an attribute of cyberspace. Creation of structural asymmetry changes the territory and rules of cyberspace. In practice, when actors create structural asymmetry they change the structure and attributes of cyberspace. In accordance with our definition of power, not all actors (states) might perceive the creation of asymmetry in the same way. 'Structural cyber asymmetry' does not define whether the asymmetry created is offensive or defensive. However, this

[66] Cf. James Hasík [183] on John Boyd and his legacy.

[67] On John Boyd's theories Cf. [184], [185, pp. 185-187], [186]; On Herbert A. Simon's 'bounded rationality', cf. [187]; And on more complex models of desicion making, cf. [188, pp. 8-12].

[68] According to Richard J. Harknett and Hasan B. Yalcin [189, p. 500]: "Structuralism, in principle, provides the opportunity of understanding human identity, motivation, and behaviour by tracing their roots to the environment in which they are all located. It is based on a belief in the shaping power of conditions over agency."

paper proposes that it is both. By studying how nation states close their national networks vis-à-vis the rest of cyberspace, it is possible to discern where and how changing the nature of objects, routes and distances and borders affect the offense-defence balance, what kind of new vulnerabilities are created, and whether they are disproportionate and exploitable. Using above described definition or framework perhaps a better understanding of the cyber battlefields of today and tomorrow on a strategic level can be achieved.

Digital territory is not shaped directly. Cyberspace is affected by technology, norms and governance, and politics. These are the means states use according to their strategy and available resources. The ways that these means are utilised is important. By studying ways and means it is possible to see where, when and how asymmetry is deliberately or unintentionally created, and also in relation to what and in what context. What this means from a methodical point of view is studying ideas, policies, strategies, regulations, and concrete projects which affect the physical, syntactic and semantic layers of cyberspace. The study of 'structural cyber asymmetry' cannot be confined to the study of documents or news items. It must also study technical solutions to be able to argue whether shaping policies are feasible. It must analyse asymmetry through formal methods like game theory to see how structures affect power relations. Furthermore, if cyberspace is a strategic domain, there should be some amount of purposeful signaling going on, as states try to build up their deterrence capabilities, however futile that might be. This is yet another object of analysis. International norms are constantly being fought over to determine whose interests are served in cyberspace and who gets to enforce those norms. This means that norm building has to be analysed as well. All in all, a certain critical perspective and multidisciplinary approach is needed to analyse 'structural cyber asymmetry.'

From a military strategic point of view, the nature of 'digital territory', and time as a dependent and related factor, do not amount to effective asymmetry. To do this they must give an advantage. It is proposed that this materialises through situation awareness, speed of decision making, freedom of action and the protection of assets. These are well established and widely accepted Western strategic level military concepts and possibly transferrable to or at least comparable with Russian (or Chinese) concepts.[69] These concepts give us ways to 'measure' (in the sense of

[69] Already Basil Liddell Hart [197, pp. 323-328] discusses the importance of freedom of action. In this paper it means the ability to conduct cyber operations and to deny the opponent its ability to conduct operations. It incorporates fire and manoeuvre as tactical level concepts. It enables the use of force against an opponent. Situation awareness and

understanding) the concrete effects of structural asymmetry. Using situation awareness, the speed of decision making, freedom of action and protection of assets as analytical categories it possible to test, even if only on a qualitative and conceptual level, how asymmetries created by shaping cyberspace affect actors. By comparing these four elements between belligerents, it is possible to make observations on disproportioned and multiplying advantages. These advantages might even affect the characteristics of cyberspace itself, like the so called ‘attribution problem’.

Potential asymmetry gains meaning in the context of the use of force. Because ‘structural cyber asymmetry’ is not something created purely in times of war, it is beneficial to study the use of cyber power for military ends during peace and wartime and between them. Particularly interesting are so called ‘grey zone’ and the ‘initial period of war’ concepts, and it is argued that ‘structural cyber asymmetry’ has three important strategic effects in these contexts.[70] They relate to deterrence, escalation control and coercion. It is argued that asymmetry through the closing of national networks provides belligerents with a definite advantage in deterrence, in controlling the way conflict evolves, and in threatening opponents from a position of strength. In this context, the shaping of cyberspace has to been seen as a long-term strategic operation that is not only aimed at winning a war but to enhance the national power of the state.

To study ‘structural cyber asymmetry’ then, it is first necessary to examine the ideas behind the shaping process and then the process itself. Then the potential effects of asymmetry have to be analysed through situation awareness, freedom of action, protection of assets and speed of decision

speed of decision making have been seen as definite components in information warfare at least from the 1990s [119]. They are essential for enabling freedom of action in cyberspace which is made of information. In cyber warfare offensive assets are separate from assets that are to be protected. The destruction of an opponent’s offensive cyber assets is difficult and perhaps pointless, but to strive for defence or resilience is not. Protection of assets has significant effects on all other concepts. It functions as a fortress by neutralising threats, maintaining control of resources and processes, and therefore providing opportunities for manoeuvre and counter attack.

[70] Cf. [135]; Hal Brands [190] describes a ‘Gray zone’: “…below the threshold of conventional military conflict and open interstate war.” The ‘Initial Period of War’ is a Russian concept that emphasises the importance of the first phase on conflict [191]. From an information warfare perspective, superiority has to be achieved and utilised for coercion and/or deterrence before the conflict breaks out [147, pp. 280-285]. In fact, Kristin Ven Bruusgard [25, p. 18] states that strategic deterrence is a continuum from neutralising threats, deterring aggression and winning confrontation. According to Dmitr Adamsky [26, p. 10] an ‘information struggle’ plays a central role in modern Russian doctrine and it is holistic, unified and uninterrupted.

making, to observe what kind of quantitative and qualitative advantages are created in cyberspace. Lastly, asymmetry has to be put in the context of cyber power and the use of force, to understand what its strategic implications are.

6 Discussion

This paper has combined ideas from different fields and from different times. It offers 'structural cyber asymmetry' as an analytical concept for the study of cyber conflicts and warfare. Most of all, it tries to capture the ongoing strategic process in cyberspace which might lead to consequencies affecting balance of power on an international level.

Already in 2011 Chris Demchak and Peter Dombrowski proposed a concept of 'Cyber Westphalia' for understanding how states delineated borders and reaffirmed state sovereignty in cyberspace [7]. They foretold that states succeeding in this project could wield military cyber power more effectively than those that fail to create needed laws and organisations. Demchak and Dombrowski were optimistic in that they saw Western nations having a material and technological advantage in this. This paper stems from a more pessimistic view. In this age of 'multi-spectrum deterrence/coercion' the advantage might well go to those who are willing to close their networks irrespective of technological challenges or economic difficulties.

What needs to be done now is to test the concept of 'structural cyber asymmetry' through case and comparative studies to see if it has, first of all, any descriptive value. Does it help us to understand what is happening in cyberspace? How does it affect our understanding of the cyber use of force? Then it must be developed further so that it can be used to explain, and even predict the creation of asymmetry and its effect on the military balance on an international level. These are, of course, tall orders, but work has alredy begun and it will be continued. If 'Cyber Westphalia' is coming, we must have concepts and tools to create a winning strategy in a 'dialectic of force.'

References

[1] M. Schmitt and L. Vihul, “International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms, Just Security,” 30 June 2017. [Online]. Available: https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms. [Accessed 19 August 2017].

[2] M. Ristolainen, "Should 'RuNet 2020' be taken seriously?," in *ECCWS*, 2017.

[3] T. Thomas, “Nation-state Cyber Strategies: Examples from China and Russia,” in *Cyberpower and National Security*, F. Kramer, S. Starr and L. Wentz, Eds., Washington, D.C., National Defense University Press, 2009, pp. 465-488.

[4] K. Giles and W. Hagestad II, “Divided by a Common Language: Cyber Definitions in Chinese, Russian and English,” in *5th International Conference on Cyber Conflict*, K. Podins, J. Stinissen and M. Maybaum, Eds., Tallinn, NATO CCD COE Publications, 2013, pp. 413-430.

[5] N. Inkster, China's Cyber Power, New York: Routledge, 2016.

[6] A. Jones and G. Kovacich, Global Information Warfare: The New Digital Battlefield, Boca Raton: CRC Press, 2016.

[7] P. Dombrowski and C. C. Demchak, “Cyber War, Cybered Conflict, and the Maritime Domain,” *Naval War College Review,* vol. 67, no. 2, pp. 71 - 96, 2014.

[8] J. Kukkola, M. Ristolainen and J.-P. Nikkarila, “Confrontation with Closed Network Nation: Open Network Society’s Choices and Consequences,” in *MILCOM 2017*, Baltimore, 2017.

[9] J. Kukkola, J.-P. Nikkarila and M. Ristolainen, "Asymmetric frontlines of the cyber battlefields," in *ICCRTS*, In Press 2017.

[10] H.-L. Lango, “Competing academic approaches to cyber security,” in *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*, New York, Routledge, 2016, pp. 7-26.

[11] J.-P. Nikkarila and M. Ristolainen, "RuNet 2020' - Deploying traditional elements of combat power in cyberspace?," in *ICMCIS*, 2017.

[12] Potomac Institute for Policy Studie, “Italy Cyber Readiness at a Glance,” 2016. [Online]. Available: http://www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf.

[13] Potomac Institute for Policy Studies , “Germany Cyber Readiness at a Glance,” 2016. [Online]. Available: http://www.potomacinstitute.org/images/CRI/CRI_Germany_Profile_PIPS.pdf. [Accessed 19 August 2017].

[14] Potomac Institute for Policy Studies , “United Kingdom Cyber Readiness at a Glance,” 2016. [Online]. Available: http://www.potomacinstitute.org/images/CRI/CRI_UK_Profile_PIPS1.pdf. [Accessed 19 August 2017].

[15] Potomac Institute for Policy Studies , “United States of America Cyber Readiness at a Glance,” 2016. [Online]. Available: http://www.potomacinstitute.org/images/CRI/CRI_US_Profile_Web.pdf. [Accessed 19 August 2017].

[16] Potomac Institute for Policy Studies, “France Cyber Readiness at a Glance,” 2016. [Online]. Available: http://www.potomacinstitute.org/images/CRI/CRI_France_Profile_PIPS.pdf.

[17] Potomac Institute for Policy Studies, “Japan Cyber Readiness at a Glance,” 2016. [Online]. Available: http://www.potomacinstitute.org/images/CRI/CRI_Japan_Profile_PIPS.pdf.

[18] Potomac Institute for Policy Studies, “Netherlands Cyber Readiness at a Glance,” 2017. [Online]. Available: http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf. [Accessed 19 August 2017].

[19] U.S. Cyber Command (USCYBERCOM), “Internet homepage,” 30 September 2016. [Online]. Available: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/. [Accessed 20 August 2017].

[20] United Kingdom, “United Kingdom government webpage,” 29 September 2013. [Online]. Available: https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit. [Accessed 20 August 2017].

[21] M. Pennetier, “Under threat, France grooms army hackers for cyber warfare, Reuters,” 5 April 2017. [Online]. Available: http://www.reuters.com/article/us-france-cyber-idUSKBN1771B2. [Accessed 19 August 2017].

[22] D. Scally, "We'll fight them on the internet: Germany's first cyber general, The Irish Times," 8 April 2017. [Online]. Available: https://www.irishtimes.com/news/world/europe/we-ll-fight-them-on-the-internet-germany-s-first-cyber-general-1.3039196. [Accessed 19 August 2017].

[23] T. Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy,* vol. 33, no. 1, pp. 148 - 170, 2012.

[24] NATO Cooperative Cyber Defense Centre for Exellence (CCD COE), "Cyber Security Strategy Documents database," 2017. [Online]. Available: https://ccdcoe.org/cyber-security-strategy-documents.html. [Accessed 19 August 2017].

[25] K. Bruusgaard, "Russian strategic deterrence," *Survival,* vol. 58, no. 4, pp. 7-26, 2016.

[26] D. Adamsky, " From Moscow with coercion: Russian deterrence theory and strategic culture," *Journal of Strategic Studies,* vol. Published online July 27, pp. 1-28, 2017.

[27] E. A. Kolodziej, "French Strategy Emergent: General Andre Beaufre: A Critique," *World Politics,* vol. 19, no. 3, pp. 417 - 444, 1967.

[28] C. Demchak and P. Dombrowski, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs,* vol. Internationa Engagement on Cyber III, pp. 29-38, 2013.

[29] W. Carlsnaes, T. Risse and B. A. Simmons, Handbook of International Relations, 2 ed., London: Handbook of International Relations, 2012.

[30] J. Baylis, J. J. Wirtz and C. S. Gray, Strategy in the Contemporary World (4th ed.), New York: Oxford University Press, 2013.

[31] S. E. Lobell, N. M. Ripsman and J. W. Taliaferro, Neoclassical Realism, the State, and Foreign Policy, Cambridge: Cambridge University Press, 2014.

[32] G. Rose, "Neoclassical Realism and Theories of Foreign Policy,"" *World Politics,* vol. 51, no. 1, pp. 144 - 172, 1998.

[33] B. Rathbun, "A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism," *Security Studies,* vol. 17, no. 2, pp. 294 - 321, 2008.

[34] I. Z. Saltzman, "Growing Pains: Neoclassical Realism and Japan's Security Policy Emancipation," *Contemporary Security Policy,* vol. 36, no. 3, pp. 498 - 527, 2015.

[35] M. E. Becker, M. S. Cohen, S. Kushi and I. P. MvManus, "Reviving the Russian empire: the Crimean intervention through a neoclassical realist lens," *European Security,* vol. 25, no. 1, pp. 112-133, 2016.

[36] D. Jordan, J. D. Kiras, D. J. Lonsdale, I. Speller, C. Tuck and W. Dale, Understanding Modern War, Cambridge: Cambridge University Press, 2008.

[37] C. S. Gray, Modern Strategy, Oxford: Oxford University Press, 1999.

[38] T. G. Mahnken, " The Future of Strategic Studies," *Journal of Strategic Studies,* vol. 26, no. 1, pp. x - xviii, 2003.

[39] H. Strachan, The Direction of War: Contemporary Strategy in Historical Perspective, New York: Cambridge University Press, 2013.

[40] P. Vennesson, ""Is strategic studies narrow? Critical security and the misunderstood scope of strategy," *Journal of Strategic Studies,* vol. 40, no. 3, pp. 358 - 391, 2017.

[41] J. S. Lantis and D. Howlett, ""Strategic Culture," in *Strategy in the Contemporary World (4th ed.)*, J. Baylis, J. J. Wirtz and C. S. Gray, Eds., New York, Oxford University Press, pp. 76 - 95.

[42] F. Doeser, "Finland, Sweden and Operation Unified Protector: The impact of strategic culture," *Comparative Strategy,* vol. 35, no. 4, pp. 284 - 297, 2016.

[43] R. Uz Zaman, Strategic Culture: A "Cultural" Understanding of War," *Comparative Strategy,* vol. 28, no. 1, pp. 68 - 88, 2009.

[44] E. Sloan, Modern Military Strategy: An introduction, New York: Routledge, 2012.

[45] J. Angström and J. Widen, Contemporary Military Theory: The Dynamics of War, New York: Routledge, 2015.

[46] E. J. Gartzke and J. R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies,* vol. 24, no. 2, p. 316 – 348, 2015.

[47] J. Arquilla and D. Ronfeldt, Cyberwar is Coming, Santa Barbara: RAND, 1993.

[48] J. Arquilla and D. Ronfeldt, In Athenas Camp,, Santa Monica: RAND, 1997.

[49] D. Kuehl, "From Cyberspace to Cyberpower - Defining the Problem.," in *Cyberpower and National Security*, Washington, D.C., National Defence Ubniversity Press, 2009, pp. 24-42.

[50] F. Kaplan, Dark Territory. The Secret History of Cyber War, New York: Simon & Schuster, 2016.

[51] B. Valeriano and R. C. Maness, Cyber War versus Cyber Realities Cyber Conflict in the International System, New York: Oxford University Press, 2015.

[52] D. A. Baldwin, "“Power and International Relations," in *A Handbook of International Relations*, W. Carlsnaes, T. Risse and B. Simmons, Eds., London, SAGE Publications Ltd: , 2013.

[53] J. Sheldon, "The rise of cyberpower," in *Strategy in the Contemporary World*, Oxford, Oxford University Press, 2013, pp. 282-298.

[54] M. Popova, "How William Gibson Coined "Cyberspace", Brain Pickings," 2014. [Online]. Available: https://www.brainpickings.org/2014/08/26/how-william-gibson-coined-cyberspace/. [Accessed 19 August 2017].

[55] B. Peters, How Not to Netwok a Nation: The Uneasy History of the Soviet Internet, The MIT Press: Cambrige, 2016.

[56] T. Rid, Rise of the Machines: A Cybernetic History, New York: W. W. Norton & Company Inc, 2016.

[57] G. J. Rattray, Strategic Warfare in Cyberspace, Cambridge: MIT Press, 2001.

[58] J. Nye, Cyber Power, Cambridge: Harvard Kennedy School, 2010.

[59] D. Betz and T. Stevens, "Cyberspace and the State: Toward a Strategy for Cyberpower," Adelphi Series 51:424, 2011.

[60] J. S. J. Nye, The Future of Power, New York: PublicAffairs, 2011.

[61] N. Choucri, Cyberpolitics in International Relations, Cambridge: MIT Press, 2012.

[62] Joint Chiefs of Staff, "Information operations (Joint Publication 3-13)," 20 November 2014. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf. [Accessed 13 October 2017].

[63] M. Libicki, Cyberdeterrence and Cyberwar, Santa Monica: RAND, 2009.

[64] R. Mattioli, "The ′States(s)′of Cybersecurity," in *Security in Cyberspace. Targeting Nations, Infrastructures, Individuals*, G. Giampiero, Ed., New York, Bloomsbury Academic.

[65] G. J. Rattray, "An Enviromental Approach to Understanding Cyberpower,"" in *Cyberpower an National Security*, Washington D.C., National Defense University Press, 2009, pp. 253-274.

[66] M. Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs, International Engagement to Cyber III,* pp. 57 - 68, 2015.

[67] M. Barnett and R. Duvall, “Power in International Politics,” *International Organization,* vol. 59, no. 1, pp. 39-75, 2005.

[68] F. Berenskoetter, “Thinking about power,” in *Power in World Politics*, London, Routledge, pp. 1-22.

[69] S. Guzzini, “The Limits of Neorealist Power Analysis,” *International Organization,* vol. 47, no. 3, pp. 443 - 478, 1993.

[70] S. Lukes, Power: A Radical View (2nd ed.), Basingstoke: Palgrave Macmillan, 2005.

[71] P. Digiser, “Fourth Face of Power,” *The Journal of Politics,* vol. 54, no. 4, pp. 977 - 1007, 1992.

[72] C. Demchak, “Cybered Conflict, Cyber Power, and Security Resilience as Strategy,” in *Cyberspace and National Security*, Washington D.C., Georgetown University Press, pp. 121-136.

[73] R. Slayton, “What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment,” *International Security,* vol. 41, no. 3, pp. 72 - 109, 2017.

[74] S. Biddle, Military Power - Explaining Victory and Defeat in Modern Battle, Princeton: Princeton University Press, 2004.

[75] B. C. Schmidt, “Realist conceptions of power,” in *Power in World Politics*, F. Brenskoetter and M. J. Williams, Eds., London, Routledge, 2007, pp. 43 - 61.

[76] T. Rid, “Cyber war will not take place,” *Journal of Strategic Studies,* vol. 38, no. 1, pp. 5-32, 2012.

[77] J. Stone, “Cyber War Will Take Place!,” *Journal of Strategic Studies,* vol. 36, no. 1, pp. 101-108, 2013.

[78] S. H. Starr, “Towards a Premilinary Theory of Cyberpower.,” in *Cyberpower and National Security*, Washington D.C, National Defense University Press, pp. 43-81.

[79] M. C. Libicki, Conquest in Cyberspace. National Security and Information Warfare, Cambridge: Cambridge University Press, 2007.

[80] J. Andress and S. Winterfeld, Cyber Warfare - Techniques, Tactics and Tools for Security Practitioners, (2nd ed.), Waltham: Syngress, 2014.

[81] North Atlantic Treaty Organization (NATO) , “Cyber Defence Pledge,” 9 July 2016. [Online]. Available: http://www.nato.int/cps/en/natohq/official_texts_133177.htm. [Accessed 19 August 2017].

[82] M. Kaldor, New and Old Wars: Organized Violence in a Global Era (3rd edition), Stanford: Stanford University Press, 2012.

[83] C. S. Gray, War, Peace and International Relations: An Introduction to Strategic History, New York: Routledge, 2007.

[84] T. Pettersson and P. Wallensteen, “Armed conflicts, 1946–2014,” *Journal of Peace Research ,* vol. 52, no. 4, p. 536 – 550, 2015.

[85] K. Okimoto, “The Cumulative Requirements of Jus ad Bellum and Jus in Bello in the Context of Self-Defense,” *Chinese Journal of International Law,* vol. 11, no. 1, pp. 45 - 75, 2012.

[86] J. S. Levy, “Review Roundtable. Clausewitz on Small War,” *The Journal of Strategic Studies,* vol. 40, no. 3, pp. 450 - 456, 2017.

[87] M. Creveld Van, The Transformation of War,, New York: The Free Press: , 1991.

[88] J. Keegan, A History of Warfare (2nd ed.), London: Pimlico, 2004.

[89] L. Milevski, The Evolution of Modern Grand Strategic Thought, Oxford: Oxford University Press, 2016.

[90] W.-M. dictionary, “"warfare",” 2017. [Online]. Available: https://www.merriam-webster.com/. [Accessed 20 August 2017].

[91] M. Dictionary, “"warfare",” 2017. [Online]. Available: www.macmillandictionary.com. [Accessed 20 August 2017].

[92] C. Dictionary, “"warfare",” 2017. [Online]. Available: dictionary.cambridge.com. [Accessed 20 August 2017].

[93] T. J. Junio, “Military History and Fourth Generation Warfare,” *Journal of Strategic Studies,* vol. 32, no. 2, pp. 243 - 269, 2009.

[94] T. X. Hammes, The Sling and the Stone: On War in the 21st Century, St Paul: Zenith Press, 2006.

[95] M. Evans, “Elegant irrelevance revisited: A critique of fourth-generation warfare,” *Contemporary Security Policy,* vol. 26, no. 2, pp. 242-249, 2005.

[96] R. C. Molander, A. S. Riddile and P. A. Wilson, Strategic Information Warfare: A New Face of War, Santa Monica.: RAND, 1996.

[97] K. Geers, Strategic Cyber Security, Tallinn: NATO CCD COE, 2011.

[98] D. E. Denning, “Is Cyber Terror Next?,” in *Understanding September 11*, New York, The New Press, 2002.

[99] M. G. Devost, B. K. Houghton and N. A. Pollard, “Information terrorism: Political violence in the information age,” *Terrorism and Political Violence,* vol. 9, no. 1, pp. 72 - 83, 1997.

[100] A. P. Liff, “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War,” *Journal of Strategic Studies,* vol. 35, no. 3, pp. 401 - 428, 2012.

[101] J. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security,* vol. 41, no. 3, pp. 44-71, 2016/17.

[102] T. C. Schelling, Arms and Influence, New Haven: Yale University Press, 2008.

[103] R. A. Pape, Bombing to Win: Air Power and Coercion in War, Ithica and London: Cornell University Press, 1996.

[104] F. Hare, “The Significance of Attribution to Cyberspace Coercion: A Political Perspective.,” in *4th International Conference on Cyber Conflict*, C. Czosseck, R. Ottis and K. Ziolkowski, Eds., Tallinn, NATO CCD COE Publications, 2012, pp. 125 - 140.

[105] J. Rivera, “Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk,” in *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, M. Maybaum, O. &. A.-M. and L. Lindström, Eds., Tallinn, , NATO CCD COE Publications, 2015, pp. 7 - 24.

[106] T. Rid and B. Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies,* vol. 35, no. 1, pp. 4-37, 2015.

[107] T. G. Mahnken, “Cyber war and Cyber warfare,” in *America’s Cyber Future Security and Prosperity in the Information Age volume II*, K. M. Lord and T. Sharp, Eds., Washington D.C., Center for New American Security, 2011, pp. 57 - 64.

[108] R. A. Clarke and R. K. Knake, Cyber War: The Next Threat to National Security and What to Do About It, New York: HarperCollins, 2010.

[109] A. Beaufre, An Introduction to Strategy, Faber & Faber: London, 1965.

[110] L. Freedman, Strategy: A History, New York: Oxford University Press, 2013.

[111] J. C. Wylie, Military Strategy: A General Theory of Power Control, Annapolis: Naval Institute Press, 2014.

[112] M. Handel, Masters of War: Classical Strategic Thought, London: Frank Cass, 1996.

[113] H. Bull, “Strategic Studies and Its Critics,” *World Politics,* vol. 20, no. 4, pp. 593 - 605, 1968.

[114] E. U. A. f. N. a. I. S. (ENISA), "Definition of Cybersecurity: Gaps and overlaps in standardisation," 1 July 2016. [Online]. Available: https://www.enisa.europa.eu/publications/definition-of-cybersecurity/at_download/fullReport. [Accessed 19 August 2017].

[115] J. Gow, "The Essence of Strategy: Constructivist Realism and Necessity," in *The Art of Creating Power: Freedman on Strategy*, B. Wilkinson and J. Gow, Eds., London, Hurst & Compandict, 2017, pp. 259 - 278.

[116] L. Milevski, "Asymmetry is Strategy, Strategy is Assymmetry," *JFQ,* vol. 75, no. 4, pp. 77-83, 2014.

[117] R. Smith, The Utility of Force: The Art of War in the Modern World, New York: Vintage Books, 2008.

[118] S. Metz and D. I. Johnson, "Asymmetry and U.S. Military Strategy L Definition, Background, and Strategic Concepts, U. S. Army Strategic Studies Institute: Carlisle," 2001. [Online]. Available: http://ssi.armywarcollege.edu/pdffiles/pub223.pdf. [Accessed 20 August 2017].

[119] A. K. Cebrowski and J. J. Garstka, "Network-Centric Warfare: Its Origin and Future," *Proceedings Magazine,* vol. 124, no. 1, pp. 28 - 35, 1998.

[120] B. Owens, Lifting the Fog of War, Baltimore: The Johns Hopkins University Press, 2001.

[121] J. Chase, "Defining Asymmetric Warfare: A Losing Proposition," *JFQ ,* vol. 61, pp. 123-126, 2011.

[122] J. Keegan, A History of Warfare, New York: Vintage Books, 1993.

[123] A. Echevarria, "Operational Concepts and Military Strength, 2017 Index of U.S. Military Strength," 2017. [Online]. Available: http://index.heritage.org/military/2017/essays/operational-concepts-military-strength/ . [Accessed 15 March 2017].

[124] V. Gerasimov, "Vystuplenie nachal'nika Genshtaba VS RF generala armii Valeriia Gerasimova na konferentsii MCIS-2016 [The speech of the chief of the General staff of the Russian Armed Forces General Valery Gerasimov at the conference MCIS-2016]," 2017. [Online]. Available: http://mil.ru/mcis/news/more.htm?id=12120704@cmsArticle . [Accessed 8 June 2017].

[125] G. Kennan, “George F. Kennan on Organizing Political Warfare April 30th 1948,” 1948. [Online]. Available: https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c. [Accessed 19 August 2017].

[126] F. E. Morgan, K. P. Mueller, E. S. Medeiros, K. L. Pollpeter and R. Cliff, Managing Escalation in the 21st Century, Santa Monica: RAND, 2008.

[127] I. Arreguin-Toft, “How the Weak Win Wars: A Theory of Asymmetric Conflict,” *International Security,* vol. 26, no. 1, pp. 93-128, 2001.

[128] B. Posen, The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars, Ithica: Cornell University Press, 1984.

[129] L. Freedman, “The Revolution of Strategic Affairs,” the Adelphi Papers 45:376, 2006.

[130] P. Mitchell, “Network Centric Warfare: Coalition operations in the age of US military primacy,” IISS, The Alelphi Papers 46:385, 2006.

[131] I. Arreguín-Toft, “Contemporary Asymmetric Conflict Theory in Historical Perspective,” *Terrorism and Political Violence,* vol. 24, no. 4, pp. 635-657, 2012.

[132] S. Biddle and I. Oelrich, “Future Warfare in the Western Pacific: Chinese Antiaccess / Area Denia, U.S. AirSea Battle, and Command of the Commons in East Asia,” *International Security,* vol. 41, no. 1, pp. 7-48, 2016.

[133] L. Simon, “Demystifying the A2/AD Buzz, War on the Rocks,” 4 January 2017. [Online]. Available: https://warontherocks.com/2017/01/demystifying-the-a2ad-buzz/. [Accessed 20 August 2017].

[134] J. Votel, C. Cleveland, C. Connett and W. Irwin, “Unconventional Warfare in the Gray Zone,” *JFQ,* vol. 80, no. 1st Quarter, pp. 101-109, 2016.

[135] J. J. Wirtz, “Life in the “Gray Zone”: observations for contemporary strategists,” *Defense & Security Analysis,* vol. 33, no. 2, pp. 106 - 114, 2017.

[136] J. A. Lewis, “National Perceptions of Cyber Threats,” *Strategic Analysis,* vol. 38, no. 4, pp. 566 - 578, 2014.

[137] C. Guitton, “Cyber insecurity as a national threat: overreaction from Germany, France and the UK?,” *European Security,* vol. 22, no. 1, pp. 21 - 35, 2013.

[138] F. D. Kramer, S. H. Starr and L. K. Wentz, Cyberpower and National Security, Washington D.C.: National Defense University Press, 2009.

[139] T. Rid and P. McBurney, “Cyber-Weapons,” *The RUSI Journal,* vol. 157, no. 1, pp. 6-13, 2012.

[140] NATO Cooperative Cyber Defense Centre for Exellence (CCD COE) , “Cyber Definitions,” [Online]. Available: https://ccdcoe.org/cyber-definitions.html. [Accessed 19 August 2017].

[141] A. Lawlor Russell, “Strategic Anti-Access/Area Denial in Cyberspace,” in *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, M. Maybaum, A. Osula and L. Lindström, Eds., Tallinn, NATO CCD COE Publications, 2015, pp. 153 - 168.

[142] C. Oehmen and N. Multari, “AiR2: Second Meeting on Asymmetry in Resilience Report on the Second Meeting on Asymmetry in Resilience for Complex Cyber Systems, U.S. Department of Energy,,” July 2016. [Online]. Available: https://cybersecurity.pnnl.gov/documents/AiR_2.0_Final_Report.pdf. [Accessed 19 August 2017].

[143] C. Oehmen and N. Multari, “AiR: Asymmetry in Resilience: Report on the First Meeting on Asymmetry in Resilience for Complex Cyber Systems,” December 2014. [Online]. Available: https://cybersecurity.pnnl.gov/documents/AiR_1.0_Final_Report.pdf. [Accessed 19 August 2017].

[144] J. Hanska, Times of war and war over time : the roles time and timing play in operational art and its development according to the texts of renowned theorists and practitioners, Doctoral Dissertation, Helsinki: National Defence University, 2017.

[145] J. B. Godwin III, A. Kulpim, K. F. Rauscher and V. Yaschenko, Eds., Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity. Policy Report 2/2014, EastWest Institute and the Information Security Institute of Moscow State University, 2014.

[146] M. Galeotti, "Heavy Metal Diplomacy: Russia's Political Use of its Military in Europe Since 2014," ECFR, 2016.

[147] T. Thomas, Russia Military Strategy: Impacting 21st Century Reform and Geopolitics, Fort Leavenworth: Foreign Military Studies Office, 2015.

[148] L. Simon, “A European Perspective on Anti-Access/Area Denial and the Third Offset Strategy, War on the Rocks,” 3 May 2016. [Online]. Available: https://warontherocks.com/2016/05/a-european-perspective-on-anti-accessarea-denial-and-the-third-offset-strategy/. [Accessed 20 August 2017].

[149] J. A. McCarthy, C. Burrow, M. Dion and O. Pacheco, “Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts.,” in *Cyberpower and National Security* , F. D. Kramer, S. H. Starr and L. Wentz, Eds., Washington D.C., National Defence University Press, 2009, pp. 543 - 556.

[150] C. Paul, Strategic Communications, Santa Barbara: Praeger, 2011.

[151] E. U. I. f. S. Studies, “EU strategic communications with a view to counteracting propaganda, European Parliament: Bryssels,” 2016. [Online]. Available: http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf. [Accessed 19 August 2017].

[152] D. J. Betz, “The more you know, the less you understand: The problem with information warfare,” *Journal of Strategic Studies,* vol. 29, no. 3, pp. 505-533, 2006.

[153] M. C. Libicki, “The Convergence of Information Warfare,” *Strategic Studies Quarterly,* vol. 11, no. 1, pp. 49 - 65, 2017.

[154] J. W. Legro and A. Moravcsik, “Is Anybody Still a Realist,” *International Security,* vol. 24, no. 2, pp. 5 - 55, 1999.

[155] C. Reus-Smith, Constructivism, in Theories of International Relations (3rd ed.), New York: Palgrave Macmillian, 2005.

[156] C. Wight, “Philosophy of Social Sciences and International Relations.,” in *A Handbook of International Relations*, London, SAGE Publications Ltd, 2012, pp. 23 - 51.

[157] S. Krasner, Structural Conflict, Berkeley: University of California Press, 1985.

[158] D. A. Baldwin, Paradoxes of Power, New York: Basil Blackwell, 1989.

[159] R. J. Art, “American foreign policy and the fungibility of force,” *Security Studies, ,* vol. 5, no. 4, pp. 7-42, 1996.

[160] D. A. Baldwin, “Force, fungibility, and influence,” *Security Studies,* vol. 8, no. 4, pp. 173-183, 1999.

[161] P. Kennedy, Ed., Grand Strategies in War and Peace, New Haven: Yale University Press, 1991 .

[162] R. S. Endresen, "Hard Power in Cyberspace: CNA as a Political Means," in *8th International Conference on Cyber Conflict: Cyber Power*, P. N., R. H. and M. Veenendaal, Eds., Tallinn, NATO CCD COE, pp. 23 - 36.

[163] V. Bufacchi, "Two Concepts of Violence," *Political Studies Review,* vol. 3, no. 2, pp. 193 - 204, 2005.

[164] I. Duyvesteyn, "Exploring the utility of force: some conclusions," *Small Wars & Insurgencies,* vol. 19, no. 3, pp. 423 - 443, 2008.

[165] M. Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review, ,* vol. 15, no. 1, pp. 105 - 122, 2013.

[166] D. L. Rousseau, T. A. Thrall, M. Schulzke and S. S. Sin, "Democratic leaders and war: simultaneously managing external conflicts and domestic politics," *Australian Journal of International Affairs,* vol. 66, no. 3, pp. 349 - 364, 2012.

[167] F. Lemieux, "Trends in Cyber Operations: An Introduction," in *Current and Emerging Trends in Cyber Operations. Policy, Strategy and Practice*, F. Lemieux, Ed., New York, Palgrave Macmillian, 2015, pp. 1-15.

[168] R. Jervis, " Cooperation Under Security Dilemma," *World Politics,* vol. 30, no. 2, pp. 167 - 214, 1978.

[169] R. Jervis, "Dilemmas About Security Dilemmas," *Security Studies,* vol. 20, no. 3, pp. 416 - 423, 2011.

[170] K. Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *Information Security Journal: A Global Perspective,* vol. 18, no. 1, pp. 1 - 7, 2009.

[171] S. J. Cimbala, "Accidental/Inadvertent Nuclear War and Information Warfare," *Armed Forces & Society,* vol. 25, no. 4, pp. 653 - 675, 1999.

[172] B. Chapman, Military Doctrine: A Reference Handbook, California: ABC-CLIO LLC, 2009.

[173] T. Benbow, "Talking 'Bout Our Generation? Assessing the Concept of "Fourth-Generation Warfare"," *Comparative Strategy ,* vol. 27, no. 3, pp. 148-163, 2008.

[174] B. Berkowitz, "Chapter seven: Warfare in the Information Age.," in *In Athena's Camp*, Santa Monica, RAND, 1997, pp. 175-189.

[175] F. G. Hoffman, "Hybrid warfare and challenges," in *Strategic Studies: A Reader*, T. G. Mahnken and J. A. Maiolo, Eds., New York, Routledge, 2014, pp. 329 - 337.

[176] B. Renz and H. Smith, Russia and Hybrid Warfare: Going Beyond the Label, Aleksanteri Papers 1/2016, Helsinki: Aleksanteri

Institute, 2016.

[177] D. A. Shlapak and M. W. Johnson, Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of Baltics, Santa Monica: RAND, 2016.

[178] E. Heginbotham, Ed., The U.S. - China Military Scorecard: Forces, Geography, and the Evolution of Balance of Power 1996-2017, Santa Monica: RAND, 2017.

[179] M. Ryan, “Full spectrum dominance: Donald Rumsfeld, the Department of Defense, and US irregular warfare strategy, 2001–2008,” *Small Wars & Insurgencies,,* vol. 25, no. 1, pp. 41 - 68, 2014.

[180] S. J. Tangredi, “CNO vs A2AD: Why Admiral Richardson is Right about Deconstructing the A2/AD Term, The Navalist January,” 10 January 2017. [Online]. Available: https://thenavalist.com/home/2017/1/8/dissecting-the-buzz-words-that-control-the-defense-debates. [Accessed 19 August 2017].

[181] United State Department of Defence (U.S. DoD), “Joint Publication 3-0: Joint Operations,” 17 January 2017. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf. [Accessed 20 August 2017].

[182] C. L. Glaser, “The Security Dilemma Revisited,” *World Politics,* vol. 50, no. 1, pp. 171 - 201, 1997.

[183] J. Hasík, “Beyond the Briefing: Theoretical and Practical Problems in the Works and Legacy of John Boyd,” *Contemporary Security Policy,* vol. 34, no. 3, pp. 583 - 599, 2013.

[184] J. A. Olsen, “Boyd Revisited: A Great Mind with a Touch of Madness,” *Air Power History,* vol. 64, no. 4, pp. 7 - 16, 2012.

[185] D. J. Bryant, “Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making,” *Military Psychology,* vol. 18, no. 3, pp. 183 - 206, 2006.

[186] F. Osinga, “ ‘Getting’ A Discourse on Winning and Losing: A Primer on Boyd's ‘Theory of Intellectual Evolution’,” *Contemporary Security Policy,* vol. 34, no. 3, pp. 603 - 624, 2013.

[187] G. Barros, “Herbert A. Simon and the concept of rationality: Boundaries and procedures,” *Brazilian Journal of Political Economy,* vol. 30, no. 3, pp. 455-472, 2010.

[188] P. K. Davis, J. Kulick and M. Egner, Implications of Modern Decision Science for Military Decision-Support Systems, Santa Monica: RAND, 2005.

[189] R. J. Harknett and H. B. Yalcin, "The Struggle for Autonomy: A Realist Structural Theory of International Relations," *International Studies Review,* vol. 14, no. 4, p. 499 – 521, 2012.

[190] H. Brands, "Paradoxes of the Gray Zone, Foreign Policy Research Institute," 5 February 2016. [Online]. Available: http://www.fpri.org/article/2016/02/paradoxes-gray-zone/. [Accessed 20 August 2017].

[191] S. J. Cimbala, "The initial period of war: Russia's Soviet heritage," *The Journal of Slavic Military Studies,* vol. 15, no. 2, pp. 59–88, 2002.

[192] R. C. Maness and B. Valeriano, "Cyber spillover conflicts: Transition from cyber conflict to conventional foreign policy disputes," in *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*, New York, Routledge, 2016, pp. 45–64.

[193] K. Friis and J. Ringsmose, Conflict in Cyber Space: Theoretical, strategic and legal perspectives, New York: Routledge, 2016.

[194] J. Gow, "The Essence of Strategy: Constructivist Realism and Necessity," in *The Art of Creating Power: Freedman on Strategy*, London, Hurst & Company, 2017, pp. 259-278.

[195] G. Lasconjarias and A. Marrone, "How to Respond to Anti-Access/Area Denial (A2/AD)? Towards a NATO Counter-A2/AD Strategy," Research Division - NATO Defense College, Rome, 2016.

[196] V. Jackson, "Tactics of Strategic Competition: Gray Zones, Redlines, and Conflicts before War," *Naval War College Review,* vol. 70, no. 3, pp. 39-61, 2017.

[197] B. H. Liddell Hart, Strategy (2nd rev. ed.), New Yrok: Meridian, 1991.

[198] M. Galeotti, Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right, Prague: Mayak Intelligence, 2016.

[199] T. Thomas, "The Evolution of Russian Military Thiught: Integrating Hybrid, New-Generation, and New-Type Thinking," *The Journal of Slavic Military Studies,* vol. 29, no. 4, pp. 554–575, 2016.

[200] O. Jonsson and R. Seely, "Russian Full-Spectrum Conflict: An Appraisal After Ukraine," *Journal of Slavic Military Studies,* vol. 28, no. 1, pp. 1–22, 2015.

[201] J. Habermas, S. Lennox and F. Lennox, “The Public Sphere: An Encyclopedia Article (1964),” *New German Critique, No. 3 (Autumn, 1974), pp. 49-55,* Vols. Autumn, 1974, no. 3, pp. 49–55, 1974.

[202] R. O. Hundley, R. H. Anderson, T. K. Bikson and R. C. Neu, The Global Course of the Information Revolution: Recurring Themes and Regional Variations, Santa Monica: RAND, 2003.

[203] Joint Chiefs of Staff, “Joint Operations (Joint Publication 3-0),” 17 January 2017. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf. [Accessed 13 October 2017].

[204] Doktrina, “Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii [Information Security Doctrine of the Russian Federation],” 5 December 2016. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. [Accessed 2017 September 22].

[205] Doktrina, “Voennaia doktrina Rossiiskoi Federatsii [Military doctrine of Russian Federation],” 25 December 2014. [Online]. Available: http://www.scrf.gov.ru/security/military/document129/. [Accessed 4 October 2017].

Epilogue – the big picture?

Juha Kukkola
Mari Ristolainen
Juha-Pekka Nikkarila

Is the closing process of the Russian network really happening? In truth, nobody knows for certain. Our scenarios and interpretations might be inaccurate. Nevertheless, we believe that we have shown that fragmentation of the global network is ongoing. Thus, we claim that our work is less damaging than arrogantly overlooking and not studying the potential closing processes. Currently, in October 2017, there are two different pieces of the puzzle that we are attempting to fit into the big picture.

The first piece is a preliminary legislative drafting project called 'About the autonomous system of the Internet' initiated primarily by *Minkomsvyaz* [the Russian Ministry of Communications and Mass Media] in 2016. Originally, this project consisted of two different and confusing proposals by *Minkomsvyaz* to update a law called 'On communications' [1] and by the FSB to update a law called 'On information, information technologies and on information security' [2].

The second piece is a draft convention 'On Cooperation in Countering Information Crime' that Russia aims, yet again, to submit for consideration to the UN General Assembly [3]. This annually repeated discussion on the international standards of cybersecurity already started in 1998 [4]. Despite differences, both of these multi-angle pieces are to some extent related to the definition and defence of Russian 'critical infrastructure' and 'critical information infrastructure'. Consequently, we wonder if these pieces, rather unexpectedly, fit together.

In general, 'critical infrastructure' refers to any system of high importance to the safety and operation of the country. Nevertheless, it is each government's definition that decides what is included in the 'critical infrastructure'. During summer 2016, when the first plans were announced to ensure the protection of the Russian 'critical infrastructure' and to eliminate the dependence of RuNet on external networks, the Russian 'critical infrastructure' was not defined. In October 2016, *Minkomsvyaz* released a draft bill that defines basic Internet infrastructure concepts such as 'autonomous system' and 'infrastructure of the Russian national segment of the Internet' and 'national .ru and .рф zone domain name registrar' from the Russian point of view. The 'Russian national segment of the Internet' is defined as 'critical infrastructure' that enables the assigning and functioning of country-code domain names (domain names that end in .ru and .рф), systems that can manage the flows of Internet traffic, and other fundamental Internet communication hardware [1]. The draft bill mandates that the state would control the RuNet's entire 'critical infrastructure', including the national .ru and .рф domains, Internet traffic exchange points (IXPs), as well as autonomous systems and networks belonging to various corporations and individuals. In this draft bill, for the first time, Russian 'critical infrastructure' is defined in detail. Nevertheless, this legal proposal was never approved nor disapproved.

In December 2016, updates to the law 'On information, information technologies and on information security' were proposed by the FSB [2]. Quite the opposite of the *Minkomsvyaz* proposal, the bill titled "On the Security of Critical Information Infrastructure of the Russian Federation" was approved on its first reading in the State Duma in January 2017. It mandates to form a special register of all companies and agencies that control objects of 'critical information infrastructure'. It was signed by Vladimir Putin in June 2017 and it will come into force in the beginning of 2018. Russian 'critical information infrastructure' defined in this law includes for instance information systems and telecommunication networks belonging to government agencies, automated control systems for technological processes in the defence industry, and includes spheres of health care, transport, communications, financial institutions, energy, and fuel. Nuclear and aerospace industries, as well as a number of other areas, are also included on this list [2].

As noted, the first legislative proposal by *Minkomsvyaz* was neither approved nor disapproved. However, in August 2017, *Minkomsvyaz* released a new legislative proposal [5]. This proposal is for the most part similar to the one released in October 2016, but it describes in more detail the ownership of the IXPs. It limits foreign ownership in any company that owns an exchange point to 20 percent and this may indicate the realization of more intense traceability of Internet connections. Moreover, it prohibits domestic Internet Service Providers (ISPs) from connecting to exchange points that belong to other states, foreign citizens, or foreign companies and organizations. It seems that *Minkomsvyaz* wishes to create a state registry for all legally permitted exchange points – in order to "ensure the integrity, stability, and safety" of the Russian national segment of the Internet [5]. This registry is needed to facilitate the collection and storage of information about IP-addresses and traffic through Russia's Internet exchange points, i.e. it would be a system for monitoring all routing information between ISPs and Russia's IP-address database. This strong control of IXPs might actually indicate how traceability of Internet connections will be implemented in practice. In order to help to minimize the problem of attribution from a closed network point of view, the traceability of connections must remain when the connection is moved from one autonomous system into another autonomous system. This legislative proposal was not approved when writing this epilogue (October 2017).

Clearly, the technical isolation ratified in legislation might ensure the "integrity, stability, and safety" of the 'critical infrastructure' of a national network. However, what else may Russia try to achieve? It may perhaps be useful for Russia's internal and external politics to define international norms on cybersecurity. Especially, to promote proposals that forbid all military action against 'critical infrastructure', i.e. against everything that one defines as 'critical infrastructure'. Particularly, it could be useful from Russia's perspective to have some inbuilt confusion between terms: 'critical infrastructure' and 'critical information infrastructure'.

The Russian draft convention 'On Cooperation in Countering Information Crime' does not allow for trans-border access to stored data without a licence from national security agencies, and also has a special paragraph dedicated to the protection of signatories' national sovereignty. The list of crimes contained in the draft convention includes, for instance, unlawful interception and changing of data, disruption to the work of computer networks, and creation of viruses and malware [3]. Before bringing up the new standards of cybersecurity for discussion in the UN General Assembly, Russia tested the proposed measures on the BRICS[1], CSTO[2] and SCO[3] countries [4]. Simultaneously with the testing and verification of the effectiveness of these measures with its allies, Russia continued to more persuasively promote the theme of cybersecurity standards in the UN.

All this could be considered as some sort of strategic line of effort where a less powerful state aims to tie the hands of more powerful states. Every state wants to fight against cybercrime and there are rules of conduct that nobody would refuse to agree to. However, the question that should be asked is who would have the ability to supervise the implementation of this kind of international agreement if it would ever become reality. It seems that, on the one hand, Russia together with its allies is conducting significant measures in order to enhance its ability to supervise and control any connections into and within its borders. And, on the other hand, by closing their national networks Russia with its allies is well prepared if there are no international agreements on cybersecurity.

[1] The BRICS countries – Brazil, Russia, India, China, and South Africa

[2] The Collective Security Treaty Organization – Russia, Armenia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan

[3] Shanghai Cooperation Organization – China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, India, and Pakistan

We might have some pieces of the puzzle missing, but we also have many pieces in our hands – when we find a place for them we might be able to see the big picture more clearly.

References

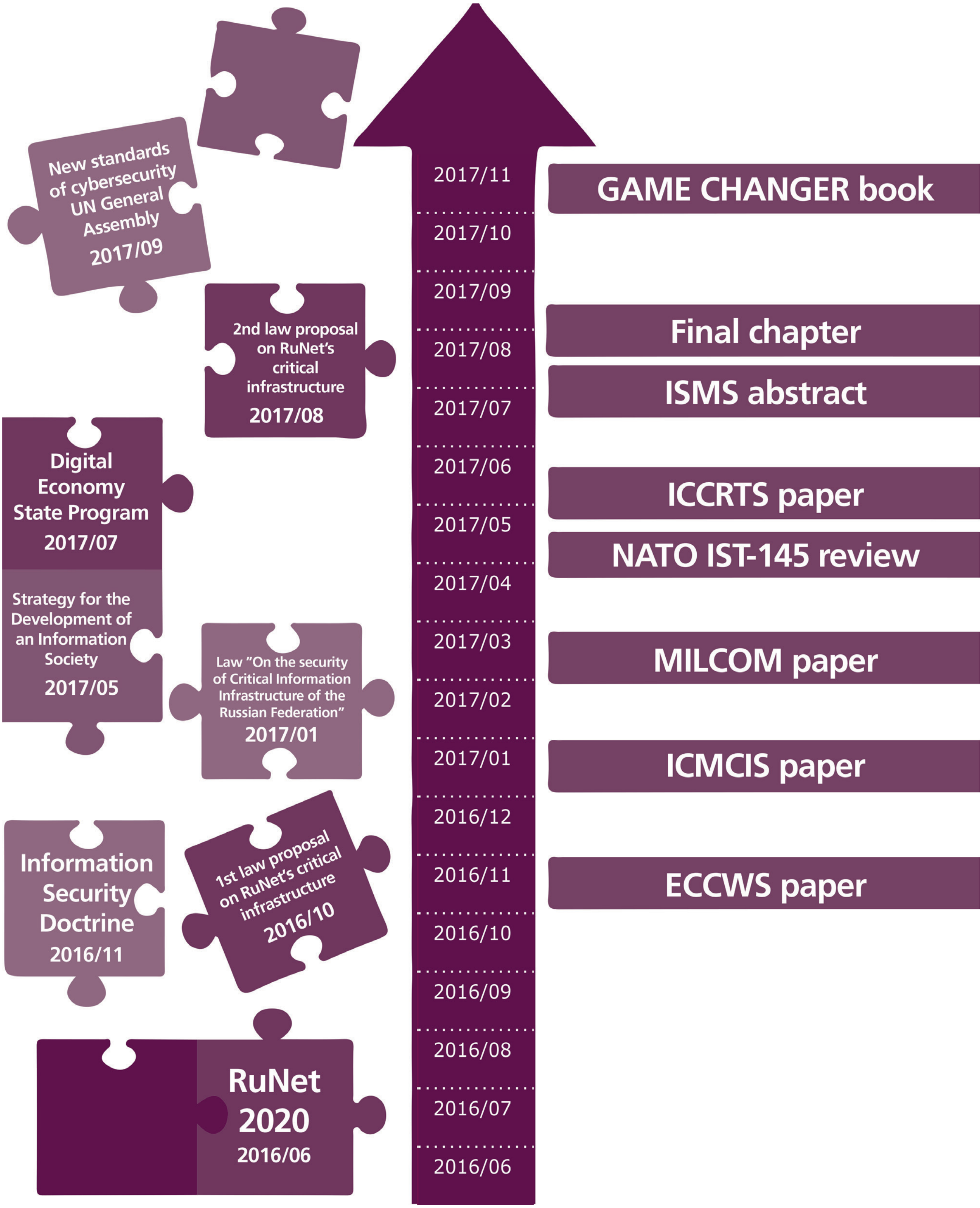
[1] Minkomsvyaz, “Federal’nyi zakon “O vnesenii izmenenii v Federal’nyi zakon “O sviazi” (Proekt) [Federal Law “On the changes to the Federal Law “On connections”],” 11 October 2016. [Online]. Available: http://regulation.gov.ru/projects#npa=58851. [Accessed 22 October 2016].

[2] "Zakonoproekt No. 47571-7: "O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii" [Bill No. 47571-7: "On the Security of Critical Infrastructure of the Russian Federation]," 2017. [Online]. Available: http://asozd2.duma.gov.ru/addwork/scans.nsf/ID/EBE024490F4C58 51432580810054D3AC/$File/47571-7_06122016_47571-7.PDF?OpenElement . [Accessed 6 March 2017].

[3] “United Nations Convention on Cooperation in Combating Information Crimes – an unofficial draft that Russia has presented and distributed for discussion in Commission on Crime Prevention and Criminal Justice,” 22-26 May 2017, May . [Online]. [Accessed 6 October 2017].

[4] A. Zabrodin, “Moskva podnimaet vopros kiberbezopasnosti na Genassamblee OON [Moscow raises the issue of cybersecurity at the UN General Assembly],” 28 August 2017. [Online]. Available: https://iz.ru/636710/aleksei-zabrodin/rossiia-podnimet-vopros-o-kiberbezopasnosti-na-ga-oon. [Accessed 4 October 2017].

[5] Minkomsvyaz, “Federal’nyi zakon “O vnesenii izmenenii v Federal’nyi zakon “O sviazi” (Proekt) [Federal Law “On the changes to the Federal Law “On connections"],” 15 August 2017. [Online]. Available: http://regulation.gov.ru/projects#npa=71277. [Accessed 2 October 2017].



New standards of cybersecurity UN General Assembly 2017/09

2nd law proposal on RuNet's critical infrastructure 2017/08

Digital Economy State Program 2017/07

Strategy for the Development of an Information Society 2017/05

Law "On the security of Critical Information Infrastructure of the Russian Federation" 2017/01

Information Security Doctrine 2016/11

1st law proposal on RuNet's critical infrastructure 2016/10

RuNet 2020 2016/06

2017/11

2017/10

2017/09

2017/08

2017/07

2017/06

2017/05

2017/04

2017/03

2017/02

2017/01

2016/12

2016/11

2016/10

2016/09

2016/08

2016/07

2016/06

GAME CHANGER book

Final chapter

ISMS abstract

ICCRTS paper

NATO IST-145 review

MILCOM paper

ICMCIS paper

ECCWS paper