RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI · ESTONIA

Analüüs

Hübriidsõja väljakutsed

Eve Hunter ja Piret Pernik

Aprill 2015

ISSN 2228-2076

Rahvusvaheline Kaitseuuringute Keskus
Toom-Rüütli 12-6, 10130 Tallinn, Eesti
info@icds.ee, www.icds.ee
Tel.: +372 6949 340
Faks: +372 6949 342

RKK analüüs
ISSN 2228-2076

Sissejuhatus

Venemaa sissetung Ukrainasse on ajendanud taas mõtlema traditsiooniliste geopoliitiliste normide ja sõjalise taktika tähenduse peale. Sel põhjusel korraldas RKK asjatundjate arutelu, et heita valgust viimastele sündmustele, eriti aga sellele, kuidas Venemaa kasutab hübriidsõda. Käesolev analüüs tuginebki suurel määral mainitud asjatundjate arutelule.

Analüütik Frank Hoffman on hübriidsõda defineeritud "riikliku konflikti surmavuse seguna irregulaarse sõja fanaatilise ja püsiva kirega".[1] Veidi pikem definitsioon kõlab järgmiselt:

> *Keerulise iseloomuga sõjakäigud, mis ühendavad endas vähese intensiivsusega tavapäraseid ja erioperatsioone, ründava loomuga küberruumitegevust ning psühholoogilisi operatsioone, mis kasutavad ühis- ja traditsioonilist meediat avaliku ja rahvusvahelise arvamuse mõjutamiseks.*[2]

Rahvusvaheline kogukond on peaaegu üksmeelselt tarvitanud Venemaa sissetungi kohta Ukrainasse mõistet "hübriidsõda". Paljud on nentinud,[3] et hübriidsõda pole iseenesest uus kontseptsioon, kuid mitmed selles kasutatavad tehnoloogiad esitavad nüüd uusi väljakutseid. Näiteks praegused arutelud küberohtude üle puudutavad, kui nimetada vaid mõningaid probleeme, kõige põhilisemate terminite defineerimist, strateegiat, informatsiooni jagamist riiklikul ja rahvusvahelisel tasandil jms. Selguse puudumine ning konkreetsete normide vähesus, kuidas käsitleda küberohte tervikuna ja Ukraina olukorda spetsiifilisemalt, on vaid täiendavalt nõrgestanud rahvusvahelist süsteemi, mida Venemaa on ära kasutanud.

Praegu puudub meil juriidiliselt või poliitiliselt määratletud eristus, mille põhjal määrata, millisel hetkel võrgusissetung ja -sabotaaž muutub sõjaks. Need küsimused valmistavad erilist muret Balti riikides, mis on ehk kõige enam ohus Venemaa agressiivse ekspansionistliku poliitika tõttu. 2015. aasta veebruari seisuga on NATO otsustanud lausa luua Eestis, Lätis ja Leedus uued lahingujuhtimiskeskused. Neid nõrkusi silmas pidades uurib analüüs hübriidsõda ja üldisemalt Venemaa poliitikat.

Strateegiliste eesmärkide täitmine

Venemaa eri taktikate ühitamine "hübriidsõja" pidamiseks on vahend laiema strateegia täitmisel. Economisti ajakirjanik Edward Lucas andis RKK 24. novembri 2014 üritusel selle eesmärkide lühiloetelu: Venemaa impeerimi taasloomine

[1] Frank G. Hoffman. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, Virginia: Potomac Institute for Policy Studies, 2007, lk 38.
[2] International Institute for Strategic Studies. *Military Balance 2015*.
[3] http://www.ft.com/intl/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html;#axzz3X2NyvJzf; http://thediplomat.com/2015/02/a-tempest-in-a-teacup-forget-hybrid-warfare/

(Novorossija ehk Uus-Venemaa), Euroopa Liidult võimaluse võtmine kontrollida energiatorujuhtmeid ning lõpuks Lääne nõrgestamine ja killustamine. Tänapäeva seisukohalt vaadatuna kajastavad need eesmärgid varasema, vähem omavahel ühendatud maailma realistlikke eesmärke.

Lääne korduv tõdemus, et majanduslik vastastiksõltuvus aitab vältida konflikte, ei avalda president Vladimir Putini mõttemaailmale mitte nii suurt mõju, kui tahetaks oodata. President Barack Obama sõnas veebruaris BuzzFeedile antud intervjuus Putini maailmavaate kohta:

> *Ma usun, et ta vaatab probleeme läbi külma sõja prisma ja seetõttu, ma arvan, on ta jätnud tähele panemata mõned võimalused, kuidas Venemaa saaks oma majandust mitmekesistada, tugevdada suhteid naabritega, olla midagi muud kui vana Nõukogude laadis agressiooni kehastus.*

Venemaa tuumarelvastuse täiendamine on kahtlemata klassikalises külma sõja võtmes jõu taotlemine, kuid vähema võimsusega taktikaliste pommide loomine kujutab endast palju häirivamat kõrvalekallet toonasest teooriast - see tähendab sisuliselt vastastikku tagatud hävitamise doktriini hülgamist.[4] Pommi kasutamist Lääne poolt peetakse tsiviilohvrite suure arvu ja järgneva humanitaarkriisi tõttu äärmiselt ebausutavaks. Üldiselt on tuumarelva kasutamine rahvusvaheliselt hukka mõistetud, kuid Moskva on jätkuvalt rõhutanud tuumarelvale toetumist, andes mõista, et ei pruugi hoolida sellest "tabust".[5] Venemaa tarvitab vanamoelist strateegiat maailmas, milles Lääs ei saa enam kindlalt väita oma moraalset üleolekut.

Taktikaline ühitamine: infosõda

Infosõjal on Venemaal teistsugune tähendus. Kui Läänes rõhutatakse "infooperatsioone", et eristada neid sõjalistest operatsioonidest, siis Venemaa doktriin kõneleb konkreetselt sõjast. Infosõda on defineeritud järgmiselt:

> *Vastasseis kahe või enama riigi vahel inforuumis kriitilise tähtsusega infosüsteemide, -protsesside ja -ressursside ning teiste struktuuride kahjustamiseks eesmärgiga õõnestada poliitilist, majanduslikku ja sotsiaalset süsteemi ning elanikkonna massiline ajupesu ühiskonna ja riigi destabiliseerimiseks ning sundimaks riiki langetama vastaspoolele kasulikke otsuseid.*[6]

Huvitav on siinjuures see, et selle definitsiooni järgi oleks Venemaa sisseimbumine Ukraina ühismeediasse ja võrku infosõda.

---

[4] James Conca. *Does Russia Think Their New Nuclear Weapons Could Win a War?* Forbes.com, 10. november 2014.
[5] Nina Tannenwald. *The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use*. International Organization 1999, 53, lk 433-468.
[6] Conceptual Views Regarding the Activities of the Armed Forces of the Russian federation in the Information Space. 2011, https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf

Psühholoogilist sõda on nimetatud Venemaa riikliku julgeoleku ja suveräänsuse peamiseks ohuks. Venemaa esimene infojulgeoleku doktriin avaldati 2000. aastal.[7] Selles on konkreetselt esitatud ülesanded elektroonilise ja seirevõime parandamiseks vastupropaganda elementide kaasamisega. Dokumendis on Venemaa Föderatsiooni infojulgeoleku tagamise peamine meetod defineeritud järgmiselt:

> *Vastupropaganda aktiveerimine eesmärgiga vältida negatiivseid tagajärgi, mis kaasnevad desinformatsiooni levitamisega Venemaa sisepoliitika kohta.*

Režiimi toetamise arvamine riigi põhihuvide hulka kindlustab, et kodanikuühiskonda käsitletakse riikliku julgeoleku operatsioonide lahutamatu osana. Praegune Venemaa doktriin ja seeläbi ka juhtkond lähtub eeldusest, et režiimi julgeolek kattub riigi julgeolekuga.[8]

Ent infosõda ei piirdu psühholoogiliste operatsioonidega. RKK vastavateemalisel üritusel tõi Ulrik Franke konkreetselt esile doktriini rõhuasetuse rünnakutele juhtimissüsteemide (C2) vastu.[9] Neis dokumentides tuuakse näiteks tõhusatest C2 küberoperatsioonidest esimene Lahesõda. Sama taktikat võis näha 2008. aasta sissetungil Georgiasse, mil halvati valitsuse, sõjaväe ja logistilised sidesüsteemid.

Üha enam peetakse Venemaad ründeotstarbelise kübervõime arendamise mõttes üheks maailma arenenumaks riigiks. USA luurekogukonna 2015. aasta aruande "Worldwide Threat Assessment" kohaselt rajab Kreml praegu Ameerika CYBERCOMi laadset küberväejuhatust ehk keskust, mis juhiks küberrünnakuid ja propagandaoperatsioone.[10] Aruanne märgib lisaks Venemaa nõndanimetatud "küberagentide" võimet imbuda sisse tööstuse juhtimiskeskustesse. Kahjurvara abil suudavad need "agendid" mõjutada vaenlase kriitilise tähtsusega taristu süsteeme.

Venemaa tsiviil- ja militaarkampaania Ukrainas

Ukrainas on infosõja teoreetilised käsitlused saanud teoks. Turbefima F-Secure aruande kohaselt paljastati 2014. aasta septembris Venemaa küberkurjategijate jõuk, mis levitas spetsiaalselt Ukraina riigiasutustele mõeldud kahjurvara BlackEnergy.[11] Kui jätta kõrvale raskused rünnaku taga olija selgitamisega, on Moskval õige mugav jätta endale eitamise võimalus ning väita, et nõndanimetatud patriootlikud häkkerid võivad tegutseda täiesti omal käel. Teiselt poolt võivad nad muidugi tegutseda ka riigi toel. Kui tegevus annab

[7] Information Security Doctrine of the Russian Federation. 2000, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument

[8] Ulrik Franke. *War by Non-Military means*, lk 19-20, http://foi.se/en/Top-menu/Pressroom/News/2015/War-by-Non-Military-means/

[9] http://www.icds.ee/et/sundmused/sundmus/rkk-s-toimus-arutelu-hubriidsojast/

[10] http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

[11] F-Secure usub, et rünnakute taga saab näha Venemaad järgmistel põhjustel: BlackEnergy on kahjurvara, mida on tuntud Venemaa põrandaaluses kübermaailmas juba alates 2007. aastast; samuti on tõendeid, et osa Ukraina riigiametnike halvamiseks mõeldud materjalist oli loodud Microsoft Office'i venekeelse versiooniga.

tulemusi, siis usutav eitamine annab Venemaale käsutusse kena puhvri, mille abil vältida konkreetseid enda vastu suunatud rahvusvahelisi samme.
Enamik Venemaa rünnakuid küberruumis on olnud loomu poolest psühholoogilised. Rünnetele on kaasa aidanud see, et viimasel viieteistkümnel aastal on ajakirjanduses hakanud üha suuremal määral domineerima riik. Nii tugev kontroll riigisiseselt ja ustavate vene kogukondade seas on võimaldanud peenemat psühholoogilist taktikat, näiteks mängimist positiivsete emotsioonide peale, andes sõduritele konkreetse näo ja demoniseerides Läänt.
NATO strateegilise kommunikatsiooni oivakeskuse aruande kohaselt on Venemaa kasutanud ühismeediat platvormina desinformatsiooni ja Lääne-vastase meeleolu levitamiseks.[12] Venemaa on lausa rajanud "trollifarme", et imbuda sisse uudiste- ja muudele ühismeediasaitidele ning vähendada teistsuguseid arvamusi väljendavate häälte mõju. Info kontrollimisel on Venemaa strateegias säilitada kontroll oma kodanike üle ja vältida teistsuguste arvamuste kõlama pääsemist väga oluline osa. 2014. aasta novembris asutas Venemaa valitsuse kontrollitava uudistekanali Sputnik News, mida Foreign Policy nimetas "propaganda-BuzzFeediks".

Küberruumi agentidel paistab olevat selge arusaam, kuidas manipuleerida inimeste tunnetega, mida seejärel saab ära kasutada arvutisüsteemide suurima nõrkuse, nimelt kasutajate mõjutamiseks. Venemaa on keskendunud pingutustele viimistleda oma relvad, seirevahendid jms nii tõhusaks, et need sobituksid täpselt kasutajate nõrkustega. Venemaalt pärit kahjurvara ja seirevahendid kasutavad sellist psühholoogilist teadmist konkreetselt ära lubamatu, sageli väga kõrge tasemega ligipääsuks riigi ja organisatsioonide siseasjadesse. Selles osas on Eesti olnud edukas näide: siin on suudetud rajada tugev kaitse, püüdes anda suurema otsustusõiguse kodanike kätte, kuid sellest hoolimata on tegu võitlusega, milles ründajatel on eeliseid. Venemaa sotsiaalmanipulatsiooni[13] viimistletus annab selgelt mõista, et seal usutakse, et informatsiooni valdamine tagab tulevastes konfliktides eelise. Lisaks teeb see väga selgeks eraandmete ulatusliku kasutamise psühholoogiliste rünnete korraldamisel.

On päris ilmne, et Venemaal on suured kogemused desinformatsiooni levitamisel, kuid Lääne tavapärane taktika ei suuda sellele vastu seista. Lääne praegune peavoolumeedia on sattunud ebatäpsuste ja ekslike reportaažide pärast tule alla. Kuid oma võimaluse pakub interneti ülilai levik ja ligipääsetavus. Hoolimata Venemaa katsetest piirata internetivabadust on Venemaa elanikel seniajani võimalus uurida muid uudisteallikaid ja nii eristada tõde väljamõeldisest. Usaldus ajakirjanduse vastu tervikuna on kõigi aegade madalaimal tasemel, mistõttu Lääne ülesanne kaitsta maailmakorda toetub üha ebakindlamale alusele, kuid kahtlemata annab vaba ja avatud internet kodanikele võimaluse tungida sügavamale, Kremli retoorika taha.

[12] NATO StratCom Center of Excellence. *Analysis of Russia's Information Campaign Against Ukraine*. 2014.
[13] US-CERT defineerib seda mõistet (inglise keeles *social engineering*) nii: "inimsuhtluse (sotsiaalsete oskuste) kasutamine ründaja poolt organisatsiooni või selle arvutisüsteemide kohta informatsiooni hankimiseks või selle informatsiooni rikkumiseks." https://www.us-cert.gov/ncas/tips/ST04-014

Kokkuvõte

1. Luure ja sissetungimine võrkudesse eelnevad tavapärasele sõjalisele sissetungile, mis annab teatava hoiatuse, enne kui konflikt jõuab jõu kasutamiseni. 2008. aasta Georgia ründamise ning Ukraina ründamise puhul kulutas Venemaa lausa aastaid riigivõrkude jälgimiseks. Iga tõend Venemaa sissetungimisest võrkudesse on teatav hoiatus, isegi kui mitte vahetust ohust.

2. Hübriidsõja pidamise tähtsaim tingimus on riigiasutuste, vabaühenduste ja eraisikute tegevuse koordineerimine.

Venemaa teostab kontrolli oma territooriumi üle viisil, mis aitab panustada loomu poolest mitmeplaanilisse hübriidsõtta. Rahvusvaheline kogukond ei pea süüdlase leidmiseks tegelema mitte ainult mitmesuguste küberruumis ja sellest väljaspool toimuvate operatsioonidega, vaid uurima ka märksa laiema valiku rühmade ja organisatsioonide suhteid.

3. Psühholoogiline sõda on ohtlik vahend, mis võib kaudselt põhjustada füüsilist kahju.

Pärast külma sõja lõppu läksid infokampaaniad Läänes moest. Inimeste käsutuses kogu maailmas on nii palju informatsiooni: raadiojaama Vaba Euroopa saadetel ei saanud olla kaugeltki samasugust mõju. Ometi on Venemaa katsed levitada desinformatsiooni olnud üllatavalt tõhusad. Sõnavabadus on oluline inimõigus, kuid mõnel juhul võib Venemaa-mõjuline ajakirjandus teha ajupesu mõjutatavatele isikutele, kes seejärel viivad ellu juba palju ohtlikumaid plaane. Psühholoogiliste vahendite kasutamisse suurte rahvahulkade manipuleerimiseks tuleb väga tõsiselt suhtuda.

Mida saaks siin ära teha? Hübriidsõda on tuleviku sõda. Kõik riigid (ja ideaalis kogu rahvusvaheline kogukond) peavad arvestama selle ebakindlusega oma poliitikas ja doktriinis. Praegune küberoperatsioone puudutavate juriidiliste ja poliitiliste vahendite puudumine muudab rahvusvahelise kogukonna sellist laadi koordineeritud rünnakute ees haavatavaks. Et kübersõja käsitlemisel pole sisuliselt mingeid pretsedente, üritab enamik riike kõrvale vaadata ega suhtu kuidagi küberruumi kuritarvitamisse. Kui agressiivsele käitumisele Ukraina võrkudes oleks reageeritud, oleks ehk Lääs suutnud asjakohasemalt ja ühtsemalt reageerida ka Venemaa füüsilisele sissetungile. Praegu aga pole õieti üldse siduvaid õigusakte, millest võiks küberoperatsioonide puhul juhinduda - pole isegi selget juriidilist konsensust, kas ründaja süsteemi tungimine on lubatav või mitte.

Seda laadi operatsioonid, mida Venemaa Ukrainas korraldab, ei ole hirmuäratavalt uued ega isegi hirmus keerulised. Pigem kasutavad need ära tõsiasja, et mis tahes operatsioonid kübermaailmas tekitavad läänemaailmas segadust. Puhkenud arutelud jätavad neile piisavalt aega ja ruumi jätkata agressiivset käitumist.