UKRAINA AVALIKU SEKTORI KOHANEMINE VENEMAA INFOSÕJAS – SOTSIAALMEEDIA KUI RELV

SOFIIA KOSTYTSKA, HANNES NAGEL, ANNE-MAY NAGEL

Võtmesõnad: Venemaa infosõda, sotsiaalmeedia, Ukraina, infohügieen, kohanemine

Ülevaade. Sotsiaalmeedia on tsiviilelanikkonna jaoks sõjaolukorras oluline suhtlusvahend, ent erinevate sotsiaalmeediaplatvormide kasutamine sõja ajal kätkeb endas ka ohte nii tsiviilelanikkonnale kui ka riigi julgeolekule. Vene sõjalise agressiooni üheks elemendiks Ukrainas on ka infosõda[1], sealhulgas sotsiaalmeedia kasutamine sõjaliste eesmärkide toetamiseks või saavutamiseks. Venemaa sõjaaegne sotsiaalmeedia relvastamine on Ukraina sõjas liikunud mittesõjaliste ja sõjaliste meetmete piirimaile, ohustades nii tsiviilelanike elu ja tervist kui ka näiteks armee positsioone.

Ukraina avaliku sektori võime neid väga tõsiseid ohte maandada on lähtunud kohanemisvõimest. Artikli eesmärk on kirjeldada Ukraina riigisektori kohanemist Venemaa infosõja võtetega sotsiaalmeedia tasandil. Artiklis käsitletakse ka Vene infosõja teooria kui doktriini kujunemist ja selle praktilist rakendamist sotsiaalmeedia militariseerimisel. Analüüsiosas kirjeldatakse Ukraina riigivõimude kohanemist läbi vastu- ja ennetussammude elanikkonna sõjaaegsest sotsiaalmeediakasutusest tulenevate ohtude vähendamiseks. Käsitletakse ka sõnavabadust ja seda, mida ütleb rahvusvaheline õigus sõnavabaduse piiramise kohta olukorras, kus ohus on riigi julgeolek.

[1] Infosõda (ja -operatsioon) on infotehnoloogia kasutamine ja haldamine eesmärgiga saavutada konkurentsieelis vastase ees (Krepinevich, 2012, p. 183).

SISSEJUHATUS

20. märtsil 2022 tabasid vene raketid Kiievis asunud Retroville'i kaubanduskeskust. Tabamusele eelnes ühe Ukraina blogija, kelle Ukraina Julgeolekuteenistus (edaspidi SBU) hiljem arreteeris, TikToki postitus. Videos oli näha kaubanduskeskuse lähedale pargitud Ukraina sõjaväe masinaid. Veidi hiljem tabasid raketid kaubanduskeskust, hukkus kaheksa inimest ja paljud lähedalasuvad elamud said kahjustada (Glover, 2022; SBU, 2022a). See on vaid üks mitmest näitest, kus pealtnäha süütu ja harjumuspärane sotsiaalmeedia kasutamine võib muutuda eluliselt ohtlikuks tsiviilelanikkonnale, kahjustada kaitsepositsioone, mõjuda halvasti moraalile või muutuda ohuks riigi julgeolekule.

Retroville'i juhtum kõneleb olukorrast, kus sotsiaalmeediapostitus on muutunud vastase tulejuhtimist abitavaks elemendiks. Selliste juhtumite puhul ei saa kõnelda sotsiaalmeedia kaudsest mõjust sõjategevusele moraali toetamise või meelsuse kujundamise abil. Sellistel juhtudel on sotsiaalmeediapostitus otseselt sõjategevust suunanud ja toonud kaasa reaalseid kaotusi. Nii on sõjas Ukraina vastu sotsiaalmeedia kui otsene tulejuht liikunud mittesõjaliste ja sõjaliste meetmete piirimaile, palju kaugemale oma infosõjas avalikku arvamust suunavast algrollist.

Venemaa sissetungi eskaleerumine täiemahuliseks rünnakuks 2022. aastal on näide kaasaegsest sõjast, kus sotsiaalmeediat kasutatakse ka militaareesmärkide saavutamiseks. Kuid Retroville'i juhtum pole ainus (Roblin, 2022; SBU, 2022b; SBU, 2022c) ning selles sõjas on asutud sotsiaalmeediat sõjavankri ette rakendama strateegilise valikuna. Seda kasutatakse ka meelitamaks indiviide kas teavet avaldama näiteks Ukraina armee positsioonide kohta (SBU, 2022d) või vastupidi, levitades sotsiaalmeedia kanalites valeuudiseid võimalike evakuatsiooniteede kohta, mis tegelikkuses osutuvad ettevalmistamise järgus olevateks õhu- ja raketirünnakute sihtmärkideks ja piirkondadeks. Olukorra tõsidust ilmestab ka vajadus tagada Ukrainale tarnitud Lääne täppisrelvade ohutus (nt HIMARS) nende positsioonide salastamise teel ehk kindlustada ka see, et nende asukoht ei saa avalikuks mõtlematu sotsiaalmeediapostituse teel. Seega on ka Eestil ja teistel, kelle jaoks Venemaa on tõsine oht julgeolekule, tarvis Ukraina kogemustest sotsiaalmeediasõjas Venemaa vastu saadud kogemustest õppida.

Siiski on infosõjale ja sotsiaalmeediale kui ühele selle rakendusviisidest oluline tähelepanu pöörata ka väljaspool Ida-Euroopat. Venemaa peab üleolekut infosõja laialdases kasutamises peamiseks võitu toovaks faktoriks nii praegustes kui ka tulevastes konfliktides (Giles & Seaboyer, 2019, p. 6). Selle olulisust ilmestab nt Krimmi annekteerimine 2014. aastal, mis on näide infosõja võimekusest ja potentsiaalist. Darczewska

(2014, p. 7) järgi on vene infosõja teooria välja töötatud selleks, et võidelda Lääne uue põlvkonna sõjadoktriinidega. Seejuures on mittesõjaliste meetmete osakaal, eriti infovaldkonnas, järsult kasvanud, ent sõja peamine sisu on endiselt armee ja toore jõu rakendamine (Chekinov & Bogdanov, 2017, p. 43).[1]

Sotsiaalmeediast lähtuvaid ohte saab aga ka kõige tõsisematel juhtudel maandada, eelkõige läbi avaliku sektori kohanemise, mille väljundiks võivad olla seadusruumi korrigeerimine, kriisikommunikatsioon ja tsiviilelanikkonna võimestamine uudsete lahenduste toel. Näiteks on Ukraina ametivõimud pidevalt inimesi hoiatanud, et nad hoiduksid mõninga info postitamisest sotsiaalmeediasse.

Sõjategevus Ukrainas annab teadlastele võimaluse uurida riigisektoris aset leidnud kohanemist – kasutatavaid meetodeid ennetamaks või leevendamaks negatiivseid mõjusid. Artikli eesmärk on kirjeldada Ukraina valitsuse kasutusele võetud avalikult kättesaadavaid vastumeetodeid alates 24. veebruarist 2022.

Artikli esimeses peatükis kirjeldatakse Vene infosõja teooriat ja selle praktilisi meetodeid. Järgnevas alapeatükis on ülevaade sotsiaalmeedia definitsioonist, kasutusest ja selle tähtsusest ning sotsiaalmeedia relvastamist. Teises alapeatükis kirjeldatakse uurimismetoodikat. Kolmandas, analüüsi alapeatükis tutvustatakse Ukraina avaliku sektori kohanemismehhanisme sotsiaalmeediast lähtuva ohuga Venemaa teise sissetungi ajal, millele järgneb arutelu.

[1] 2017. aastaks oli vene militaarajakirjas Военная Мысль ilmunud 13 artiklit, mis mõjutasid oluliselt seda, kuidas Lääne analüütikud mõistavad Vene sõjandust ja sõjapidamisviise. Artiklid andsid ülevaate sellest, milline on Venemaa mõtteviis, kuidas ja milliste võimetega kavatsetakse sõtta minna (Thomas, 2020, p. 2).

1. VENE INFOSÕJA TEOORIAST JA KOHANEMISEST

Kuigi infosõjal on Venemaal nii teoorias kui praktikas pikk traditsioon, pärineb selle juriidiline algus 1942. aastast, mil NSV Liidu Kaitse Rahvakomissari käskkirjaga nr 0271 muudeti 2. võõrkeelte instituudi lääne keelte sõjaline teaduskond punaarmee võõrkeelte sõjaliseks instituudiks (Barsukov, 1997, p. 203). Sealse õppekava õppeainet (vn) *спецпропаганда* ('eripropaganda') (Grigas, 2016, p. 45–46) kasutati Bouwmeesteri (2017, p. 138) järgi mitme valdkonna edendamiseks, nagu nt blokeeriv mõjutamine ja surve avaldamine. Mõlemal on oluline roll järgmistes propaganda sotsiaaltehnilistes printsiipides:

- massiivse ja pikaajalise mõju põhimõte;
- soovitud ja manipuleeritud teabe uskumise põhimõte, nt (vn) дезинформция (desinformatsioon);
- eeldatava ilmselguse põhimõte ja emotsionaalse agitatsiooni põhimõte, nt (vn) агитпроп (agitprop).

Kuigi eripropaganda eemaldati õppekavast 1990. aastatel pärast NSV Liidu lagunemist, taastus selle õpetamine aastal 2000. On põhjust eeldada, et eespool nimetatud tehnikad on mitte ainult jäänud kasutusse, vaid neid on pidevalt õpetatud, kuid ka ajakohastatud vastavalt infosõja praegustele vajadustele.

Darcewska (2014, p. 8) kohaselt toetub vene infosõja kontseptsioon suuresti traditsioonilistele nõukogude psühholoogilise sõjapidamise kogemustele, ent Venemaa on selle tehnikaid järjepidevalt muutnud ja täiustanud, võttes sealjuures arvesse ka uusi meediavahendeid ja sotsiaalvõrgustikke. Sestap kujutavad praegused vene infosõja operatsioonid endast pigem moodsat, internetiajastu versiooni juba väljakujunenud nõukogudeaegsest reaalsuse taastamise taktikast, kusjuures Venemaa on tunnistanud, et infotehnoloogiaid saab kasutada tulevastes konfliktides (Ajir & Vailliant, 2018, p. 75). Selle ajaloolise külje kohta on Pipes (1995, p. 313) tabavalt märkinud:

> Bolševike uuendus seisnes selles, et propagandale omistati riigis keskne koht: kui varem kasutati propagandat reaalsuse ilustamiseks või moonutamiseks, siis kommunistlikul Venemaal sai propagandast asendusreaalsus.

Venemaa kübersõda[2] on loonud tõsiseid pretsedente ka Eestis. Esimesed ulatuslikud küberrünnakud DDoS-teenuste vastu toimusid Eestis 2007. aastal peamiste riigiasu-

[2] Kübersõda hõlmab rahvusriikide või valitsusväliste osalejate tegevust, mis kasutab küberrelvi, et tungida arvutitesse või võrkudesse eesmärgiga sisestada, rikkuda ja/või võltsida andmeid; häirida või kahjustada arvutit või võrguseadet; või tekitada kahju ja/või häirida arvuti juhtimissüsteeme (Krepinevich, 2012, pp. 15–16).

tuste ja e-teenuste infrastruktuuride vastu (Herzog, 2011, lk 52). Kuigi rünnakud olid osa laiemast poliitilisest konfliktist Eesti ja Venemaa vahel, puudus selle rünnaku ajal sotsiaalmeedia laialdane kasutamine. Nimelt nähti sotsiaalmeediat enne 2010. aastat pigem ühishuvidega inimeste ühendamise vahendina, hiljem on rõhuasetus nihkunud kasutajate loodud sisu tekitamisele ja jagamisele (Aichner *et al.*, 2021, p. 220). Seega on sotsiaalmeedia praeguses rakenduses potentsiaalse infosõjapidamise pinnasena noorem kui kübersõja pidamine.

Venemaa hakkas uutele, veebipõhistele sõjapidamise meetoditele keskenduma pärast 2008. aasta sissetungi Georgiasse (Thomas, 2010, p. 277). Üks haru Vene relvajõudude vastu suunatud kriitikast lähtus piiratud jõudlusest infovaldkonnas, mis viis ettepanekuni luua spetsialiseerunud infoväed (Giles & Seaboyer, 2019, p. 8). Infovägede loomise üks ajend oli ka pärast Georgia invasiooni vastu võetud infoühiskonna arengustrateegia, milles nähti vajadust uue riikliku julgeolekustrateegia järele seoses Georgia invasiooni käigus saadud õppetundidega (Bilanishvili, 2021, p. 1). Lisaks sellele ilmus 2008. aastal Vene regionaalmeedias (Thomas, 2010, p. 281) sarnase sisuga artikleid, milles heideti ette Venemaa kaotust 2008. aasta infosõjas, aga esile toodi ka soovitusi:

> Presidendi otsusega tuleks moodustada spetsiaalsed organisatsiooni-, juhtimis- ja uurimisüksused teabeagressiooni vastu võitlemiseks. Tuleks luua infoväeosad, mis koosneksid riiklikust ja sõjalisest uudismeediast, Venemaa vajadustele ja huvidele reageerivatest inimestest, kes reageerivad kriisile. Informatsiooniväed tegeleksid kontrollvõrkude strateegilise analüüsi, vastuluuretööga, operatiivsete varjamismeetmetega, infoturbe küsimustega ning oma meeste ja varustuse turvalisusega. /…/ Infovägede personaliks oleksid diplomaadid, eksperdid, ajakirjanikud, kirjanikud, publitsistid, tõlkijad, operaatorid, kommunikatsioonitöötajad, veebidisainerid, häkkerid ja teised. (nt [*Anon*.], 2008; Panarin, 2008, pp. 1, 10)

See ettepanek on realiseerunud (nt Russia Today, RIA Novosti, Voice of Russia, Internet Research Agency loomisega) ja isegi ületatud, kuna ka sotsiaalmeedias peituvaid võimalusi on uuritud ja kasutusele võetud.

2014. aastaks ilmnesid märgid sellest, et infooperatsioonid, mis võivad hõlmata laiaulatuslikku sotsiaalpsühholoogilist manipuleerimist, on saanud vene sõjadoktriini osaks (Blank, 2014). Thomase (2010, pp. 293–294) kohaselt prognoositi, et 2020. aastate alguseks on märgata tähelepanuväärset arengut Venemaa infosõjapidamise kõigis kolmes harus – välises, sisemises ja sõjalises. Praegu ongi infosõda Venemaa jaoks lai ja kõikehõlmav mõiste, mis hõlmab suurt valikut tegevusi, kuhu kuulub vaenulik tegevus, milles kasutatakse informatsiooni kui vahendit, sihtmärki või operatsioonide valdkonda (Giles & Seaboyer, 2019, lk 6).

Seega on infosõja pidamist sõltuvalt tegevuse sihtmärgist vähemalt kahte tüüpi:

- infopsühholoogiline sõjapidamine (nt relvajõudude ja elanikkonna mõjutamine), mis toimub loomuliku konkurentsi tingimustes st pidevalt;
- infotehnoloogiline sõjapidamine (nt püüd mõjutada tehnilisi süsteeme, mis võtavad vastu, koguvad, töötlevad ja edastavad teavet), mida viiakse läbi sõdade ja relvastatud konfliktide ajal (Kvatškov, 2004).

Ka Chekinov & Bogdanov (2017, pp. 44–45) on märkinud, et infosõda on uutes tingimustes igasuguse hübriidsõja ilmingu lähtepunktiks – sh tegevused, milles kasutatakse laialdaselt massimeediat ja võimaluse korral globaalseid arvutivõrke (nt blogid, erinevad sotsiaalvõrgustikud jne). See hõlmab paratamatult ka sotsiaalmeediat. Lukas & Pomeranzevi (2016, p. 6) sõnul on teabe kui relva kasutamise keerukus ja intensiivsus Venemaal märkimisväärselt kasvanud.

Eelmainitud uuendustest lähtuva ohuga toimetuleku võtmeks Läänes on avaliku sektori kohanemine. Püüd muutusi mõista ongi üks tähtsamaid kaasaegse valitsetuse väljakutseid (Van Assche *et al.*, 2014, p. 3), mistõttu võib ka vaadet organisatsioonidele jagada kaheks:

- organisatsioonid kui korra tagamise instrumendid (Law, 1993) või;
- organisatsioonid kui määramatuse keskkonnas korra tagajad läbi muutumise (Weick, 2009).

Seejuures on korda eelkõige võimalik tagada kohanemise abil. Murray (2009) järgi on innovatsiooni ja kohanemisvõime vahel olulised erinevused, kuna rahuajal esitab aeg uuendajale väheolulisi väljakutseid – võivad puududa küll märkimisväärsed ressursid, ent aega on ideede ja arusaamade kujundamiseks, katsetamiseks ja hindamiseks (*ibid*., p. 357). Sõjas on olukord aga vastupidine, lahingus osalejatel on tavaliselt enam ressursse kui aega ja neil, kes taotlevad keset konflikti ulatuslikke muudatusi doktriinis, tehnoloogias või taktikas, on kohanemiseks piiratud võimalused (*ibid*., p. 358). Samas tuleb arvesse võtta asjaolu, et organisatsiooni kohanedes võib seda teha ka vastane.

2. DESINFORMATSIOON JA OHTLIKUD VÕLTSINGUD

Teave on võimas relv, seda eriti tänu digitehnoloogiatele, mis võimaldavad kontrollida andmevooge ja saavutada ülemaailmset katvust. Kuid digitaalajastul oleme kohanud olukordi, kus teave muutub veelgi ohtlikumaks – näiteks kui seda moonutada, infoga manipuleerida ja seda sõjapidamises kasutada. Desinformatsioon ei ole mitte ainult osa geopoliitilisest või sõjalisest strateegiast, see on ka elanikkonna psühholoogilise

mõjutamise vahend. Paanika külvamine või mahasurumine, moraali tõstmine või nõrgendamine, ilmsete faktide eitamine mis tahes julmuste õigustamiseks – desinformatsioon on nende eesmärkide saavutamiseks universaalne vahend.

ÜRO eriraportöör on rõhutanud 2021. aasta aruandes arvamus- ja sõnavabaduse õiguse edendamise ja kaitse kohta, et „valeinfot võivad rakendada osalejad, kellel on risti vastupidised eesmärgid", nimetades järgnevaid teabega manipuleerimise viise:

- desinformatsioon (valeinfo tahtlik levitamine);
- väärinfo (valeinfo levitamine tahtmatult);
- tõe delegitimatsioon selle nn valeuudiseks tembeldamise teel (Khan, 2021, p. 3).

See klassifikatsioon on täpne, kui seda kohaldada riikide sõjaolukorras võetud meetmete spektrile, eriti kui arvestada Venemaa riiklikult toetatud valeinformatsiooni strateegiat. Maailmameedias on avaldatud arvukalt faktikontrolle, analüüsimaks Venemaa väiteid Ukraina bio- (nt Myers, 2022, p. 1) ja tuumarelvade (nt Oliker, 2022) väljatöötamise kohta kuni alusetute väideteni, et Butša veresaun (nt Al-Hlou *et al*., 2022, p. 10) või Mariupoli sünnitusmaja pihta antud raketilöögid ja selle tagajärjed (Benedek *et al*., 2022, pp. 46–47) on lavastatud. Venemaa desinformatsiooni leviku tõkestamiseks on loodud ka spetsiaalseid veebilehti, nagu evsdisinfo.eu ning debunk.eu.

Tõhus ennetamine ja desinformatsiooni vastu võitlemine võib nõuda keerulisi riiklikult toetatud meetmeid, eriti sõja tingimustes. Näiteks eespool nimetatud ÜRO 2021. aasta aruanne sisaldab desinformatsiooniga võitlemiseks soovitusi, mis on väärtuslikud nii rahuajal kui ka täiemahulise sõja tingimustes, näiteks:

- mitme sidusrühma dialoog ja partnerlus;
- riigi läbipaistvuse suurendamine, nt avalikustades proaktiivselt ametlikke andmeid nii internetis kui ka väljaspool (selline ametlik avalikustamine relvastatud konflikti tingimustes nõuab siiski erilist ettevaatust);
- digitaalse kirjaoskuse edendamine (autorid rõhutavad, et arvesse tuleks võtta ka sotsiaalmeedia kirjaoskust).

Olulisi soovitusi, mida tuleks kaaluda, on Euroopa Liidu tasandil liikmesriikidele koostatud ka varem. Näiteks on Euroopa Komisjon (2018, pp. 36–37) esile toonud vajadust tugevdada kodanike meedia- ja teabekirjaoskuse toetamist ja suurendada teadusasutuste rahastamist, mis haldavad faktikontrollijatele avatud innovatsioonikeskusi või uurimislaboreid. Kuigi soovitused anti enne Venemaa agressiooni Ukraina vastu, on nende rakendamine sõjaolukorras endiselt oluline.

Desinformatsiooni vastu võitlemine on muutunud nii Ukraina ametivõimude kui ka kodanikuühiskonna oluliseks missiooniks. 11. märtsil 2021 asutas Ukraina riiklik julgeoleku- ja kaitsenõukogu (presidendi nõustav organ) desinformatsiooni vastase võitluse keskuse (Ülemraada, 2021). Asutus valmistab Ukraina riikliku julgeoleku- ja kaitsenõukogu jaoks ette analüütilisi dokumente ja uuringuid Venemaa desinformatsiooni kohta, andes samal ajal ukrainlastele konkreetseid soovitusi valeuudiste kohta. Lisaks loodi eraldi Strateegilise Kommunikatsiooni Keskus (edaspidi SKK), mis on üks desinformatsiooni vastu võitlemise mehhanismidest riigi ja kodanikuühiskonna ühiste jõupingutuste abil (Ukraina kultuuri- ja teabepoliitika ministeerium, 2021).

3. SOTSIAALMEEDIA – SUHTLUSPLATVORMIST VENEMAA RELVAKS

Sotsiaalmeediat kasutatakse uuringutes üldiselt katusmõistena veebiplatvormide (nt foorumid, blogid, sotsiaalmängud, videote jagamine jne) kirjeldamiseks (Aichner *et al.*, 2021, p. 215). Kuigi kogu sotsiaalmeedia hõlmab mingit digitaalset platvormi, ei ole siiski kõik, mis on digitaalne, tingimata sotsiaalmeedia (Manning, 2014, p. 1158). Viimast määratlevad kaks peamist omadust: see võimaldab mingis vormis osalemist ja vastavalt oma osalusspetsiifikale ka interaktsiooni (*ibid*.).

Peale suhtlemise ja enda kogemuste jagamise kasutatakse sotsiaalmeediat ka mitterahumeelsetel viisidel, nt valimistesse sekkumiseks (Stavridis & Weinstein, 2017), vaktsineerimisvastaseks tegevuseks (Broniatowski *et al.*, 2018) jne. Sotsiaalmeedial on meie igapäevaelus üsna suur roll ning see kehtib ka kriiside ja sõdade puhul. Inimesed kasutavad sotsiaalmeediat kontakti hoidmiseks ka loodusõnnetuste (Yates & Partridge, 2015), terrorirünnakute (Cheong & Lee, 2010) ja revolutsioonide (Lotan *et al*., 2011) ajal. Choudhury *et al.* (2014, p. 3563) kohaselt pöörduvad inimesed ka relvakonflikti korral teabe saamiseks sotsiaalmeedia poole, viimane kehtib eriti juhul, kui traditsioonilised meediakanalid ei tööta. Samas pakub sotsiaalmeedia mõningast rutiini ja võimalust hoida kontakti ka nt okupeeritud aladel.

Lähtuvalt sotsiaalmeedia kasutamisest sõjas toob McCauley (2016, p. 86) välja, et Venemaa on oma mõjuvõimukampaaniate tõhustamiseks arendanud infosõjavõimekust, sealhulgas pettustegevust ja sotsiaalmeedia relvastamist. Ajir & Vailliant (2018, p. 75) rõhutavad samuti, et erilise tähtsusega on propaganda levitamine sotsiaalmeedias, mida võib vaadelda ka kui infooperatsiooni ja kübersõja sõlmpunkti. Prier (2017) on ka analüüsinud uute infosõja platvormide relvastamist, märkides, et analüütikud on USAs aastaid hoiatanud nn küber-Pearl Harbouri eest.

Desinformatsiooni taktikat (avaliku) arvamuse eksitamiseks on küll kasutatud ka enne, aga selle edu tõenäosus ja sellest tulenev negatiivne mõju on siiski suurenenud just sotsiaalmeedia ajastul. Mõned vanemad tehnikad (nt agitprop-tehnikad, nagu paraadid, vaatemängud, plakatid, filmid jne) kinnistusid 1920. aastatel (Kenez, 1986, pp. 251–260) pärast kommunistliku partei agitatsiooni ja propaganda osakonna loomist (Brown, 2013, p. 5) ning jätkusid kuni 1991. aastani.

Kuigi NSV Liidu lagunemisega eemaldati agitpropist kommunistlik ideoloogia, on selle erinevatele meetoditele lisandunud uus kultuurilis-religioosne ideoloogia – Русский мир, mis omakorda on arenenud koos tehnoloogia ja ühiskonna arenguga ülekantuna ka sotsiaalmeediasse. Agitprop ja desinformatsioon koos peamiste (internetipõhiste) meediaväljaannetega, nagu Russia Today ja Sputnik, mängivad endiselt võtmerolli Vene narratiivide ühendamisel (Van Herpen, 2016, pp. 76–77).

Kui sotsiaalmeedias peituvad sõjaajal märkimisväärsed ohud, siis tekib paratamatult küsimus kohanemise võimalikkusest – kaaluda tuleks nii tsiviilelanikkonna kui ka kaitsejõududes tegevate isikute sotsiaalmeediakasutuse piiramise võimalikkust ja vajadust nii tsiviilelanikkonna kui riigi julgeoleku kaitseks. Kohanemise üks väljund võib olla ka sõnavabaduse piiramine.

3.1. Sõnavabadus ja sotsiaalmeedias avaldatava info piiramine

Harjumuseks saanud sotsiaalmeediakasutus võib sõjaoludes omandada uue tähenduse. Näiteks sõjakuritegude tunnistaja käes olev kaameraga mobiiltelefon võib muutuda oluliseks tõendite kogumise ja avaldamise vahendiks tulevaste kohtumenetluste jaoks. Kuid kuna ka sotsiaalvõrgustikud on vaenlase tähelepanu ja ehk isegi kontrolli all, tuleks mistahes infot avaldades arvestada, et isegi väga keerulistes olukordades on olemas tundlik või salastatud teave, mille jagamist piiravad reeglid.

14. aprillil 2022 andis Ukraina parlament välja deklaratsiooni sõnavabaduse tähtsuse, ajakirjanike ja meedia tegevuse tagatiste kohta sõjaseisukorra ajal, mille kohaselt:

> /…/ agressorriigi näitel oleme näinud, milliseks võib muutuda karmi propaganda ja sõnavabaduse puudumise tingimustes elava riigi ühiskond. Julm, manipuleeriv propaganda on üks peamisi põhjusi, mis ajab riigi sõjani /.../ Ülemraada rõhutab, et riigi üks peamisi ülesandeid peaks olema sõnavabaduse tagatiste kindlustamine /.../ Ukraina riigil ei ole õigust kopeerida agressiivse riigi totalitaarset praktikat (Ülemraada, 2022a).

Sellest hoolimata, nagu rahvusvaheline üldsus on laialdaselt kinnitanud, on õigus sõnavabaduse riikliku julgeoleku küsimustes piiramisele.

Sõnavabadus on kirjeldatud kodaniku- ja poliitiliste õiguste rahvusvahelise pakti (edaspidi ICCPR) artiklis 19. Vastavalt kodaniku- ja poliitiliste õiguste konventsioonile peab sõnavabaduse mis tahes piirang või piiramine olema sätestatud seadusega, teenima ühte loetletud eesmärkidest ja olema vajalik selle eesmärgi saavutamiseks. Eelkõige on ICCPR artikli 19 lõikes 3 sõnavabaduse piiramise põhjuste (eesmärkide) hulgas loetletud riikliku julgeoleku kaitse koos avaliku korra, rahvatervise või kõlbluse kaitsega (ÜRO, 1966, p. 171).

Lisaks võib sõna- ja teabevabadust piirata riikliku julgeoleku kaitsmise eesmärgil „ainult kõige tõsisematel juhtudel, kui on tegemist otsese poliitilise või sõjalise ohuga kogu rahvale“ (Hussain, 1994, p. 12). Riikliku julgeoleku kaalutlustel põhinevad kitsendused on õigustatud, kui „tegelik eesmärk ja tõendatav mõju on kaitsta riigi olemasolu või territoriaalset terviklikkust jõu kasutamise või selle ohu eest või tema võimet reageerida jõu kasutamisele või selle ohule“ (ARTICLE 19, 1996, p. 8). Euroopa inimõiguste konventsiooni (edaspidi EIÕK) artikkel 10 tunnistab riiklikku julgeolekut kui võimalikku alust teatavate sõnavabaduse piirangute kehtestamiseks (EIÕK, 2010).

Riigisaladuste hoidmine on tähtis rahulikel aegadel, aga see muutub veelgi olulisemaks sõja tingimustes, kus nt vägede liikumisest kui avalikult nähtavast sündmusest teadasaajate hulka ei saa piirata näiteks riigisaladuse loa olemasoluga. Seega on tasakaalu leidmine sõnavabaduse tagamise (sh avalikkuse teavitamise sõjakuritegudest) ning riigi julgeoleku kaitsmise vahel üks olulisemaid küsimusi, millega tuleb kaasaja sõdades sotsiaalmeediaajastul tegeleda.

4. METODOLOOGIA

Artikli metodoloogia põhineb dokumendianalüüsil baseeruval uurimisel, mis on tõhus meetod kvalitatiivsete juhtumiuuringute puhul (Bowen, 2009, p. 29) loomaks nähtuse või sündmuse üksikasjalikud kirjeldused (Stake, 1995).

Boweni (2009, pp. 29–30) järgi kasutatakse dokumendianalüüsi erinevatel põhjustel:

- anda andmeid selle konteksti kohta, milles uuringus osalejad tegutsevad;
- dokumentides sisalduv teave võib viidata mõnele küsimusele, mida tuleb esitada;
- dokumendid pakuvad täiendavaid uurimisandmeid ja võivad olla väärtuslikuks täienduseks teadmiste baasile;
- dokumendid annavad võimaluse jälgida muutusi ja arengut;

- dokumente saab analüüsida, et kontrollida järeldusi või kinnitada muudest allikatest saadud tõendeid.

Dokumendianalüüs hõlmab artiklis nii veebilehtedel, sotsiaalmeedias kui mobiilirakendustes leidunud teabe analüüsimist. Näiteks Ukraina valitsusasutuste veebi- ja sotsiaalmeediakanalites, sh mobiilirakendustes avaldatud teavet analüüsitakse ja esitatakse asjakohaseid näiteid lähtuvalt uurimiseesmärgist. See võimaldab kaardistada ka vahendeid, mida kasutatakse mõjude maandamiseks sotsiaalmeedia infosõjas.

Mittetehniline kirjandus, nt aruanded koos igat liiki dokumentidega (Merriam, 1988, p. 118), on potentsiaalsed empiiriliste andmete allikad kolme valdkonna puhul, mida analüüsitakse tähenduse avamiseks, mõistmiseks ja oluliste arusaamade leidmiseks:

- seadusandliku ruumi kohandused Ukrainas lähtuvalt sotsiaalmeedias varitsevatest ohtudest;
- kriisikommunikatsioon tsiviilelanikele, ennetamaks keelatud info levitamist sotsiaalmeedias;
- tsiviilelanike võimestamine luureinfo kogumises sotsiaalmeedia ja rakenduste kaudu.

Järgnevalt on esitatud loetelu Ukraina valitsusasutuste veebilehtedest ja sotsiaalmeedia kontodest (Facebook ja Telegram), milles kajastatud sisu on artiklis analüüsitud vahemikus juuli kuni august 2022:

- Ukraina Ülemraada veebileht (seaduste analüüs vahemikus 23. märts kuni 20. juuli 2022);
- SBU ja ministeeriumid, täpsemalt Kultuuri ja teabepoliitika ministeerium, Digitaalarengu ministeerium, kaitseministeeriumi teabeagentuur ArmyInform; pressiteated ja soovitused perioodil 15. juuli kuni 30. juuli 2022;
- Ukraina riiklik statistikaamet;
- Veebiuudiste portaalid (Interfax-Ukraine ja ArmyInform veebilehti on analüüsitud perioodil 1. august kuni 10. august 2022).

Samas tuleb märkida, et dokumentide analüüsi ei ole alati kasulik ette võtta, kuna dokumentidele on omane hulk piiranguid, mille hulka võivad kuuluda ebapiisav detailsus, vähene kättesaadavus ja erapoolik selektiivsus (Bowen, 2009, p. 32). Siiski peetakse neid piiranguid tavaliselt pigem võimalikeks puudusteks kui suurteks takis-

tusteks ning arvestades eelkõige selle tõhusust ja kulutasuvust, kaaluvad dokumendianalüüsi eelised piirangud üles (*ibid*.).

5. ANALÜÜS

Ukraina ametivõimud on elanikkonda sotsiaalmeediakasutusest lähtuvate ohtude maandamiseks eri viisidel hoiatanud, et nad hoiduksid kindla teabe avaldamisest sotsiaalmeedias. Ukrainas kehtivad sõja esimestest päevadest ka asjakohased õigusaktid, mis muuhulgas sätestavad tundliku teabe avaldamisega (sh sotsiaalmeedias) kaasnevad tagajärjed.

5.1. Seadusandliku ruumi kohandused Ukrainas lähtuvalt sotsiaalmeedias varitsevatest ohtudest

3. märtsil 2022 andis Ukraina armee juhtkond välja käskkirja armee ja meedia koostöö kohta, milles sisaldub loetelu teabest, mille avalikustamine võib negatiivselt mõjutada armee tegevust sõjaseisukorra ajal (URJÜ[3], 2022). Loetelu sisaldab 17 eri tüüpi teavet – alates sõjaväeüksuste nimedest ja asukohtadest kuni personali arvu ja kavandatud või tühistatud sõjaväeoperatsioonideni.

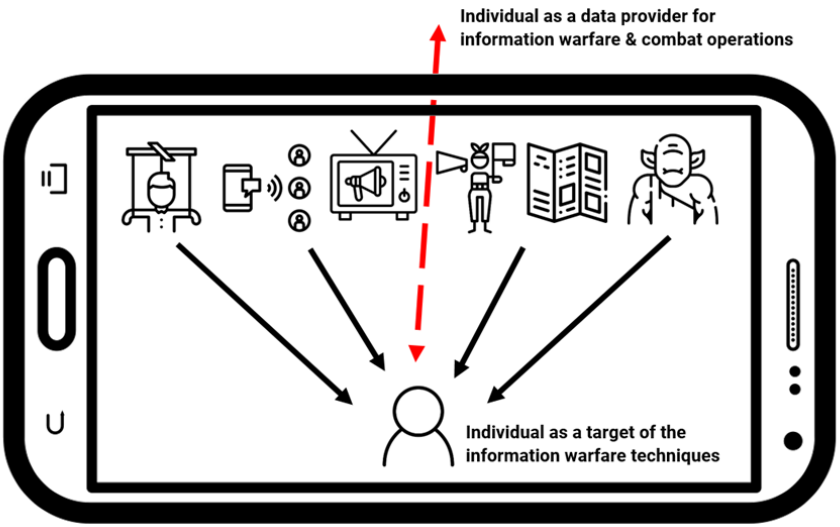
Ülemraada (2022b) võttis 23. märtsil 2022. aastal vastu asjakohased muudatused Ukraina kriminaalkoodeksis, millega kehtestati kriminaalkaristus Ukrainale tarnitud relvade või laskemoona ning Ukraina vägede asukoha või liikumise kohta käiva teabe avalikustamise eest. Ukraina kriminaalkoodeksi artikli 1142 kohaselt on sellise teabe levitamine õiguspärane ainult juhul (*ibid.*), kui seda on eelnevalt vabalt kättesaadavana avaldanud armee peastaap, kaitseministeerium, kaitseministeeriumi luurepeadirektoraat, SBU või partnerriikide ametlikud allikad. Vastasel juhul ei tohi sellist teavet avalikustada, rikkumiste korral kohaldatakse isikute suhtes kriminaalkaristusi:

- 3–5 aasta pikkust vangistust, kui avalikustatakse teavet Ukrainale tarnitud relvade või laskemoona kohta;
- 5–8-aasta pikkust vangistust, kui avalikustatakse teavet Ukraina vägede asukoha või liikumise kohta;
- 8–12 aasta pikkune vangistus on ette nähtud juhul, kui selline teave avaldatakse konspiratiivselt või eesmärgiga teavitada otseselt agressiivset riiki (selle esindajaid) (Ülemraada, 2022b).

[3] Ukraina Relvajõudude Ülemjuhataja (edaspidi URJÜ).

5.2. Kriisikommunikatsioon tsiviilelanikele, ennetamaks keelatud info levitamist sotsiaalmeedias

Kui armeed puudutava teabe avalikustamise oht tundub üsna ilmne, tuleb arvesse võtta veel üht aspekti – igasuguse teabe avaldamine vene rakettide kahjustatud hoonete tabamuste, koordinaatide, asukoha kohta või vastavad fotod ja videod võivad samuti ohtlikuks osutada ning aidata vaenlasel oma tulejuhtimist parandada. Joonisest 1 lähtub, et indiviid võib sotsiaalmeedia infosõjas olla nii info sihtmärk kui ka info edastaja.



Joonis 1. Sotsiaalmeedia duaalne kasutamine Venemaa propaganda ja luureandmete kogumise vahendina Ukrainas

Lisaks tundliku info avaldamise tagajärgede formuleerimisele seadusandluses on oluline koht ka elanikkonna informeerimisel sõjaaegse ohutu ja seaduspärase sotsiaalmeediakäitumise osas. Ukraina riigiasutused ja kohalikud omavalitsused on andnud soovitusi meediategevuse kohta sõja ajal, näiteks Ukraina kaitseministeeriumi teabeagentuur (ArmyInform, 2022a) jagas järgnevaid juhiseid kodanikele, blogijatele ja meediale (vt joonis 2–4):

Ukraina Riiklik Side- ja Teabekaitseteenistus (edaspidi SSSCIP) (2022) on rõhutanud, et umbes 80% luureandmetest kogutakse avalikest allikatest (sh sotsiaalmeediast), ja jaganud seda ning muud lisainfot oma ametlikel sotsiaalmeediakanalitel nagu Telegram. SBU (2022e) töötas välja ka juhised sõjaväelastele sotsiaalvõrgustike kasutamiseks (vt joonis 7), kus soovitatakse sõjaväelastel minimeerida juurdepääsu oma isikuandmetele, kasutades sotsiaalvõrgustike privaatsussätteid, hoiduda geograafilisi koordinaate või muid sarnaseid asukohatunnuseid sisaldavate andmete postitamisest, samuti mitte kasutada Venemaa sotsiaalvõrgustikke ja internetiplatvorme (nt Vkontakte, mail.ru, yandex.ru, rakendus Dembel).

Kuigi valeuudiste ja -info eesmärk on kahjustada riigi kui terviku kuvandit ja tajumist, kujutab spetsiifiline väärinfo olukorra kohta väiksemates piirkondades, näiteks humanitaarkoridoride või aktiivse võitluse aladel, otsest ohtu inimeste elule. Näiteks hoiatas SKK (2022) 26. mail tsiviilelanikke ka Vene nn roheliste koridoride valeinfo eest – marsruutide eest, mida reklaamiti ohutute evakuatsioonikoridoridena, ent mis tegelikult olid varitsused põgeneda soovijatele.

Lähemalt sai uuritud ka ametlikke riigiasutuste kontosid ja kanaleid jäljendavate võltskontode kasutamist. Näiteks hoiatas SBU (2022f) 25. aprillil *Stop Russian war* liba-*bot*'ide eest, mille agressor lõi vastukaaluks peagi pärast Ukraina riigi *bot*'i käivitamist, mille eesmärk oli võimaldada kodanikel avaliku teenuse kaudu teavitada Ukraina armeed vaenlase vägedest või sõjategevusest. Libakontode käivitamise põhjused võivad jääda ebaselgeks, kuigi on lihtne ennustada, et käsitletud juhul oleksid sellised liba-*bot*'id venelaste jaoks viis, kuidas tuvastada digitaalseid partisane okupeeritud territooriumidel, takistades samal ajal Ukraina armeed saamast inimestelt vajalikku luureinfot vaenlase vägede paiknemise või tegevuse kohta.

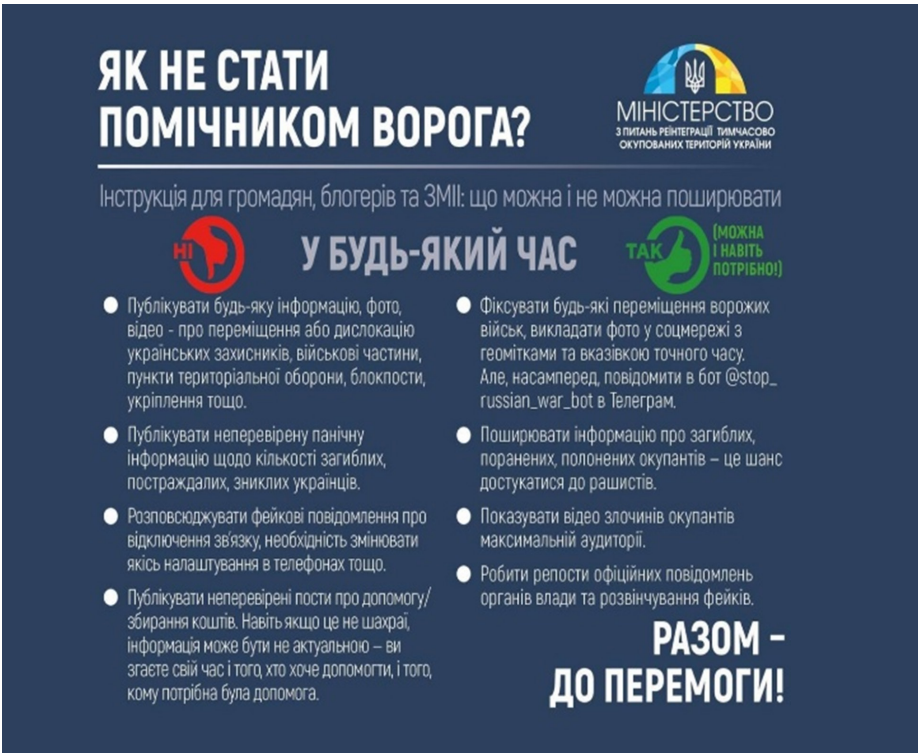
5.3. Tsiviilelanike luureinfo kogumises võimestamine läbi sotsiaalmeedia ja rakenduste

2019. aastal võttis Ukraina juhtmõtte *riik nutitelefonis* all kasutusele programmi *digitaalne riik*, rakendades e-valitsemise vahendeid ja arvukaid elektroonilisi teenuseid koos selleks loodud Digitaalarengu ministeeriumiga. Digitaliseerimisreformi raames käivitati üks edukamaid projekte, valitsustarkvara *ДІЯ* (DIIA), mis tähendab ukraina keeles tegevust ja on lühendatud vorm (ukr) держава *і я* ('riik ja mina'). Venemaa täiemahulise invasiooni algusest on DIIA, nagu ka teised riigi poolt välja töötatud rakendused ja vahendid, mänginud olulist rolli ukrainlaste infohügieeni ja turvalisuse tagamisel.

DIIA on multifunktsionaalne vahend (nii nutitelefonirakendus kui ka valitsuse teenuste veebiportaal)[4] ning mõeldud eelkõige selleks, et anda tuvastatud kodanikele vahetu juurdepääs oma ametlikele dokumentidele (nt pass, juhiload, COVID-sertifikaadid jt dokumendid). Arvestades riigis ümberasustatud inimeste, pagulaste ja nende inimeste suurt arvu, kellel võib puududa ligipääs paberdokumentidele sõjategevuse- ja purustuste tõttu, on juurdepääs oma isikut tõendavatele dokumentidele otse nutitelefonis osutunud eluliselt oluliseks.

2022. aasta märtsi alguses ajakohastati DIIAt uute funktsioonidega, mis on ukrainlaste käsutuses jätkuva sõja väljakutsetest ja nõuetest lähtuvalt. Üheks selliseks kasulikuks vahendiks on teenus eVorog (*єВорог* ehk 'eVaenlane'), mille eesmärk on võimaldada kodanikel võimalikult lihtsalt teavitada Ukraina relvajõudusid vaenlase vägedest. Olulise sammuna lisati DIIAsse Telegrami *bot*'i eVorog (@evorog_bot) link, mis lihtsustab ukrainlaste jaoks otse Ukraina armeele Venemaa väeosade, sõjatehnika ja sõjalise tegevuse kohta teabe saatmist, kui seda on mõnes riigi osas märgatud. Seega saab iga inimene, kes soovib armeed aidata, jagades teavet vaenlase vägede või tegevuse kohta, teha seda suhteliselt kiiresti ja lihtsalt.

[4] Vt lähemalt https://diia.gov.ua ja https://go.diia.app.



IGAL AJAL / ÄRA

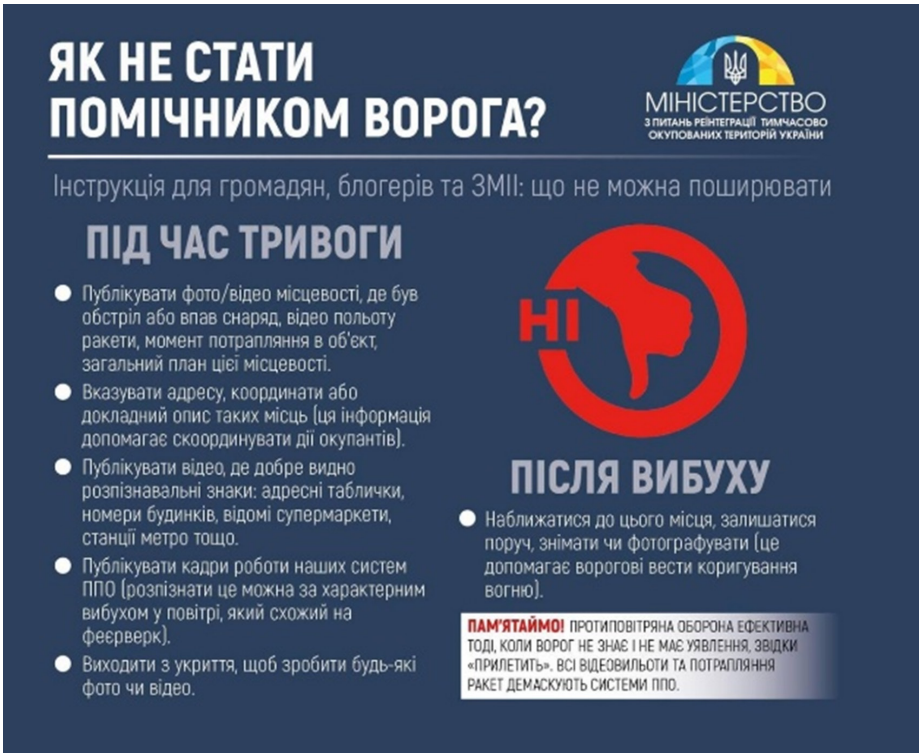
- avalda mis tahes teavet, fotosid, videoid Ukraina kaitsjate, sõjaväeüksuste, territoriaalkaitseüksuste, julgeolekukontrollipunktide, kindlustuste jne liikumisest või asukohast;
- avalda kontrollimata paanilist teavet hukkunute, vigastatute, kadunud ukrainlaste arvu kohta;
- levita valesõnumeid side sulgemise, mobiilsideühenduse seadete muutmise vajaduse jms kohta;
- avalda kontrollimata postitusi abi/annetuste tegemise vajaduse kohta. See ei pruugi olla pettus, kuid teave võib olla vananenud – raiskad nii nende aega, kes tahavad aidata, kui ka nende, kes vajasid abi.

TEE NII (lubatud ja isegi vajalik!):

- dokumenteeri kõik vaenlase vägede liikumised, postita nende fotod koos geomärgistega ja täpse ajaga sotsiaalmeediasse. Kõigepealt teavita Telegrami boti: @stop_russian_war_bot;
- levita infot hukkunud, vigastatud, kadunud okupantide kohta – see on võimalus jõuda venelasteni;
- jagage videoid okupantide kuritegudest maksimaalsele publikule;
- jagage riigivõimude ametlikke sõnumeid ja valeinfo ümberlükkamisi.

Koos kuni võiduni!

Joonis 2. Juhised tsivilistidele (ArmyInform, 2022a)



ÕHUHÄIRE AJAL / ÄRA

- avalda fotosid/videoid rakettidelt tabamuse saanud või tulistatud kohtadest, videoid lendavatest rakettidest, raketilöökide hetkedest, territooriumi kaardistamisest;
- märgi selliste kohtade täpset aadressi ja koordinaate (see teave aitab okupantidel oma tegevust koordineerida);
- avalda videoid koos identifitseerimistunnustega: aadressid, majade numbrid, tuntud supermarketid, metroojaamad jne;
- avalda meie õhutõrjejõudude tööd (saab identifitseerida konkreetse plahvatuse järgi õhus, sarnaselt ilutulestikuga);
- lahku varjendist, et teha fotosid või videoid;
- pärast plahvatust tule plahvatuse koha lähedale ega jää lähedale, filmi ega pildista (see aitab vaenlasel paremini sihtida).

Pidage meeles! Õhutõrjevahendid on tõhusad, kui vaenlane ei tea, kust see võidakse käivitada. Kõik videod õhutõrjerakettidest paljastavad õhutõrjejõud.

Joonis 3. Juhised tsivilistidele (ArmyInform, 2022a)

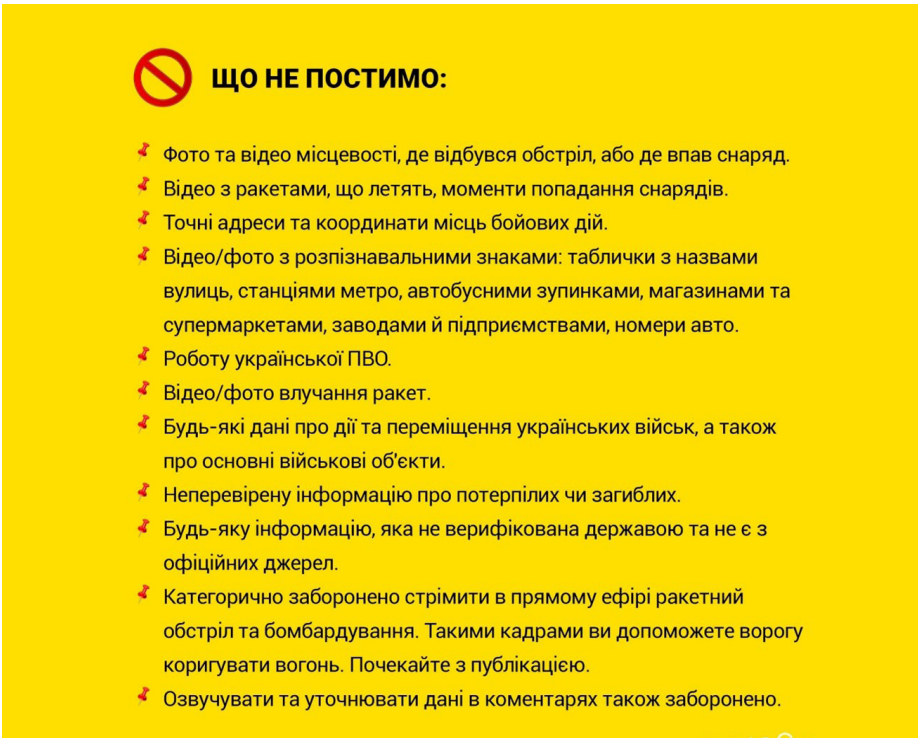
PÄRAST ÕHUHÄIRET

- Dokumenteerige hoonete ja infrastruktuuri kahjustused lähifotodel, nii et ümbritsev on kaadrist väljas. Vältige tuntud objekte kaadris.
- Jagage selliseid fotosid sotsiaalvõrgustikes, saatke need maailma meediale, riigijuhtidele jne.
- Kui jagate fotot kahjustustest, ärge märkige objekti täpset nime (näiteks „lasteaed nr 222“ asemel „lasteaed“).

Ettevaatust! Videoid raketi- või raketilöökidest ei tohiks üldse avaldada. Eriti ohtlikud on need, kui neid avaldatakse kohe pärast rünnakut – nii parandate vaenlase sihtimist veebi vahendusel.

Joonis 4. Juhised tsivilistidele (ArmyInform, 2022a)

Samuti koostasid paljud Ukraina eraõiguslikud meediaettevõtted üksikasjalikud käsiraamatud teabeohutuse kohta, milles tuletatakse kodanikele meelde, et nad peaksid hoiduma teatud informatsiooni postitamisest (Panchenko, 2022). Tsiviilisikute teavitamiseks koostati ka lihtsustatud keelunimekirjad (vt joonis 5–6):



MIDA MITTE POSTITADA:

- Fotod ja videod kohtadest, mida tabavad raketid või mida tulistatakse.
- Videod lendavatest rakettidest, raketilöökide hetkedest.
- Võitlustegevuste täpsed aadressid ja koordinaadid.
- Videod/fotod koos identifitseerimistunnustega: tänavate sildid, metroojaamad, bussipeatused, kauplused ja supermarketid, tehased ja ettevõtted, autode numbrimärgid.
- Õhutõrjejõudude töö.
- Videod/fotod õhurünnakutest.
- Mis tahes andmed Ukraina vägede tegevuse ja asukoha kohta, samuti suuremate sõjaliste objektide kohta.
- Kinnitamata teave ohvrite või hukkunute kohta.
- Mis tahes teave, mida riik ei ole kontrollinud ja mis pärineb mitteametlikest allikatest.
- Rangelt keelatud: õhurünnakute, pommitamiste ja raketirünnakute voogedastus internetis. Selline teave aitab vaenlasel parandada oma sihtimist. Oodake enne avalikustamist.
- Teabe avalikustamine või parandamine kommentaarides.

Joonis 5. Sõja ajal rangelt keelatud avaldada (Ukraina kultuuri- ja teabepoliitika ministeerium, 2022)

Kuidas saate aidata inforindel

Maailm peab teadma tõde. Mõni aeg pärast rünnakut võite avaldada internetis kõik okupantide kuriteod: hävinud arhitektuur, majad, vigastatud inimesed.

Avaldage lähifotosid, et vaenlane ei saaks asukohta tuvastada.

Hankige teavet ametlikest allikatest, lükake valeinfo ja võltsingud ümber, rääkige rahvale tõtt.

Kas teil on teavet okupantide ja vaenlase sõjatehnika asukohtade kohta?

Teavitage relvajõudusid: Telegram vestlusrobot @evorog_bot.

Joonis 6. Sõja ajal rangelt keelatud avaldada (Ukraina kultuuri- ja teabepoliitika ministeerium, 2022)

Ärge töötage vaenlase suurtükiväe vaatlejana!

Kui te ei taha aidata vaenlasel hävitada meie linnu ja külasid:

- Ärge nimetage sotsiaalvõrgustikes, avalikes kõnedes ja kommentaarides meediale täpseid sihtmärke ja tabatud objekte.
- Ärge tehke avaldusi õhutõrje puudumise kohta konkreetsetes rindeosades ega märkige vastavaid geograafilisi koordinaate.
- Ärge tehke avalikke avaldusi, mis puudutavad ainsat turvalist marsruuti linna sisenemiseks, jagades selle marsruudi üksikasju.
- Ärge öelge ega kirjutage: rakett tabas kooli nr. 7. Parem öelda: rakett tabas elamurajooni linnas X.
- Ärge öelge: rakett oli suunatud raudteejaama vastu, kuid tabas lähedal asuvat haiglat.
- Ärge öelge: rakett tabas lennuvälja lähedal asuvat ladu. Pärast sellise teabe jagamist võib olla teine või isegi kolmas rakett, mis kindlasti tabab lennuvälja.

Miks on see oluline?
80% sõjaliseks otstarbeks mõeldud luuretegevusest saadakse avatud allikatest. Sellised avaldused võimaldavad vaenlasel parandada oma tulejuhtimist teie linnades.

Joonis 7. Sotsiaalmeedia kasutamise juhised kaitse- ja jõustruktuuride esindajatele (SSSCIP, 2022)

Lisaks üksikasjalikele juhistele on loodud ka video ettevaatusabinõude soovitustega vaenlase vägede jäädvustamisel; eelkõige soovitatakse kodanikel filmida diskreetselt ja ohutus kauguses, samuti kustutada kõik materjalid ja *bot*'i ajalugu pärast kõigi vajalike andmete saatmist. Seda videot jagasid hiljem ka teised Ukraina meediakanalid. Kuid peale eVorogi teenuse on ukrainlastele kättesaadavad ka teised ametlikud riigi poolt käivitatud Telegrami *bot*'id.

Esimestel päevadel pärast Venemaa taaskordset rünnakut käivitas SBU näiteks teise Telegrami *bot*'i @stop_russian_war_bot, et inimesed saaksid teavitada märgatud Venemaa sõjatehnikast ja vägedest, samuti igasugusest teabest vaenlase agentide (saboteerijate) kohta (SBU, 2022g). Erinevalt eVorogist ei nõua see *bot* DIIA kaudu isiku tuvastamist, et saata teavet vaenlase vägede kohta. Muud teenused, mis võeti kasutusele ametliku riikliku rakenduse DIIA raames, hõlmavadki tasuta juurdepääsu riiklikule televisioonile ja raadiole nutitelefonis, mis on eriti oluline kahjustatud sidevõrkudega piirkondades (IU, 2022a; IU, 2022b) ja ajutiselt okupeeritud territooriumidel.

Sõjaaegsetele funktsioonidele lisaks jätkab DIIA ka põhitegevust digitaalse mitmekülgse riigiplatvormi tööriistana, võimaldades näiteks ettevõtjatel hõlpsasti esitada maksudeklaratsioone ja maksta makse, aga ka pakkuda ukrainlastele eDemokraatia küsitluskeskkonda.

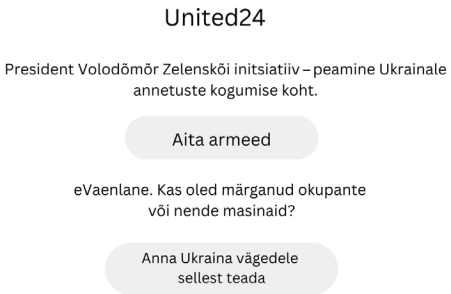
Üks oluline aspekt, mida sõja ajal arvesse võtta, on ka õhuhäirete süsteem. Kuigi enamikus Ukraina linnades on tänavatele paigaldatud õhusireenid, oli mõnes piirkonnas nende seadmete katvus ebapiisav ja inimesed ei kuulnud õhurünnakute häireid. Võimalike raketilöökide avastamise tingimustes on pommivarjendisse jõudmiseks oluline aga iga minut. Selle probleemi lahendamiseks töötati lisaks infrastruktuuriparandustele (tänavasireenide heli reguleerimine, nende võrgu laiendamine) valitsuse toetusel välja nutitelefoni rakendus, mis sisaldab sisseehitatud sireeni ja piirkonna valikut (Ukraina valitsusportaal, 2022). Rakenduse kasutajaliides on lihtne ja kasutajasõbralik, et eri taustaga ja eri vanuserühmade inimesed saaksid selle funktsioonides hõlpsasti navigeerida. Lisaks käivitati ametlik Telegrami *bot* @air_alert_ua, et teavitada inimesi käimasolevatest õhuhäiretest. Lisaks Ukraina valitsuse algatustele[5] on ka kodanikuühiskond andnud suure panuse ukrainlaste turvalisuse tagamisse, näiteks on vabatahtlike meeskondade poolt välja töötatud arvukad veebikaardid Ukraina õhuhäirete kohta.

Sarnaseid kohaliku tasandi algatusi on rakendatud alates kohalike omavalitsuste Telegrami kanalitest, mis sisaldavad koheseid teateid õhurünnakuohu kohta, kuni õhurünnaku hoiatusteadete rakendamiseni olemasolevate vahendite uue funktsioo-

[5] Vt lähemalt https://alerts.in.ua, https://alarmmap.online ja https://map.ukrainealarm.com.

nina. Näiteks täiustati rakendust Kyiv Digital, mida varem kasutati ühistranspordi jaoks (QR-piletite ostmine ühistranspordiga sõitmiseks, parkimisarvete maksmine), lisades sellele varjendite kaardi ja õhurünnakute teateid.[6] Varjendite kaardid töötati välja kõigi Ukraina piirkondade jaoks ja lingid neile avaldas kaitseministeerium (ArmyInform, 2022b) kohe pärast Venemaa rünnaku algust.

Lisaks sellele on Ukraina riiklik hädaabiteenistus käivitanud rakenduse miinide ohukaardiga. Rakendus[7] sisaldab potentsiaalselt ohtlike (võimalike mineeritud) alade kaarti, samuti edastab teateid, kui kasutaja läheneb ohtlikule objektile. Lisaks on rakenduses sisseehitatud kataloog plahvatusohtlike objektide fotode ja kirjeldustega ning vahend, mille abil saab Ukraina riiklikule hädaabiteenistusele kahtlastest objektidest teatada.



Joonis 8. Nutitelefoni rakendus United24 (Ukraina Hääl, 2022)

[6] Vt lähemalt https://kyiv.digital/start.
[7] Vt lähemalt https://apps.apple.com/ua/app/minefree/id1624507845?l.

KOKKUVÕTE

Venemaa infosõda on pika traditsiooniga valdkond ja selle kasutamine sotsiaalmeedias on uus normaalsus nii rahuajal kui ka otsese sõjalise agressiooni korral, nagu seda on kogenud Ukraina. Venemaa viib sotsiaalmeedias läbi ka infosõjategevust, mille eesmärk on nii oma narratiive toetava teabe levitamine kui ka tsiviilisikute otsene mõjutamine, aga ka erinevatest sotsiaalmeedia valdkondadest olulise teabe hankimine raketilöökide edukuse või Ukraina armee kohaloleku või liikumise kohta. Seega on Ukraina vastu suunatud Vene infosõda kahepoolne vahend, mida kasutatakse nii soovitud teabe levitamiseks propaganda eesmärgil kui ka sellise teabe hankimiseks, mis parandab otseselt näiteks kas sihtimist või Ukraina-meelsete kogukonnaliikmete märkamist okupeeritud aladel.

Informatsiooni mõtlematu postitamine on reaalsete näidete põhjal osutunud ohtlikuks tsiviilisikutele, taristule, armeele ning seeläbi ka riigi julgeolekule. Et leevendada mõtlematust sotsiaalmeediakäitumisest tulenevaid võimalikke ohte tsiviilisikute (ja sõjaväelaste) poolt, on Ukraina riigivõimud sotsiaalmeediast lähtuva ohuga kohanenud ning:

- viinud läbi teavituskampaaniaid keelatud ja lubatud infost sotsiaalmeedias;
- viinud sisse asjakohased muudatused õigusaktides ja kriminaalkoodeksis, mis võimaldavad määrata karistusi juhul, kui tundlikku teavet tehakse kättesaadavaks, seejuures olenemata asjaolust, kas see juhtus kogemata või tahtlikult;
- rakendanud sotsiaalmeedia ja rakenduste võimalusi tsiviilelanike võimestamiseks, näiteks luureandmete kogumisel (vaenlaste vägede asukohad, vägede liikumised jne).

Viimane punkt kõneleb sellest, et kuigi sotsiaalmeedia ja nutiseadmete sõjaaegsest kasutamisest tulenevad küll märkimisväärsed ohud, saab Ukraina näitel neid kasutada ka vajaliku teabe levitamiseks. Ukraina on käivitanud spetsiifilised *bot*'id ja lisanud vastavad võimalused ka valitsusrakendusse DIIA. Kodanikke julgustatakse aktiivselt vaenuvägede tegevusest teada andma, kuid seda vaid turvalisel viisil. Elanikele antakse ka konkreetseid juhised, kuidas end oluliste luureandmete kogumise käigus mitte ohtu seada. Samuti julgustab riik kindlat liiki teabe (nt sõjakuritegude, infrastruktuuri kahjustamise või tsiviilisikute vigastuste kohta) jagamist, kuid jällegi – väga konkreetses kontekstis ja viisil, mis ei avalda teavet, mida vaenlase väed saaksid ära kasutada.

Artiklis käsitleti lühidalt ka sotsiaalmeedia kasutamise reguleerimist sõja ajal sõnavabaduse perspektiivist lähtuvalt. Kuigi sõnavabadus on üks vaba ja demokraatliku

ühiskonna nurgakive, lubavad nii ICCPR kui ka EIÕK sõnavabaduse piiramist teatud juhtudel, millest üks on oht riigi julgeolekule. Sotsiaalmeedia ajastul, kus igaüks, kellel on sobiv seade ja internetiühendus, võib saada tahtmatult ja teadmatult vaenulike jõudude informaatoriks ning halvemal juhul lahingtegevuse tulejuhiks, on sõnavabaduse piiramine sotsiaalmeediapostitustes üks ainsatest võimalikest vahenditest vältimaks tundlike andmete avaldamisega kaasnevaid võimalikke negatiivseid tagajärgi.

Võttes arvesse Ukraina sõjaaegset kogemust sotsiaalmeedia rindel, soovitavad autorid, et riigid, kel on ajalooline Venemaa agressiooni kogemus ning kes seisavad jätkuvalt silmitsi võimaliku Vene Föderatsiooni sõjalise ohuga, uuriksid, kuidas Venemaa on kasutanud sotsiaalmeediat mitte ainult propaganda ja desinformatsiooni eesmärgil, vaid ka luureteabe hankimiseks, kasutades sealjuures tsiviilisikute teadmatust. Viimase mõistmine ning tsiviilelanike ja sõjaväelaste informeerimine sotsiaalmeedia kasutamise ohtudest sõja ajal enne reaalse agressiooni algust võib aidata vältida taristu ja elutähtsa varustuse kahjustamist, tsiviilelanike vigastusi ja isegi surmajuhtumeid.

Mõned küsimused tekivad ka siis, kui vaatleme Venemaa infosõda sotsiaalmeedias ja võimalikke viise selle mõju piiramiseks nn ohutsoonis asuvates (Venemaaga piirnevates) riikides. Eesti puhul tõstatub näiteks küsimus: millise ministeeriumi pädevusse kuuluks inimeste sõjaaja sotsiaalmeedia kasutamise alase teavitamise korraldamine? Lisaks: kas ja kuidas on Eesti relvajõud selles valdkonnas koolitatud, kas see on osa ajateenistuses läbitavast treeningust? Ja lõpuks üldisem küsimus: milline vastutus ja millises ulatuses on infosõja tingimustes sotsiaalmeedia platvormidel, nagu Facebook? Kas oleks mõeldamatu, et sotsiaalmeediaplatvormid töötaksid välja tehisintellekti lahenduse võltsingute, desinformatsiooni või tundlike andmete avastamiseks ja keelustamiseks juba enne postitamist?

Ühtlasi juhivad autorid tähelepanu asjaolule, et Ukraina avalikkusel oli sõjaaegse infohügieeniga teataval määral võimalik kohaneda 2014. aasta esimesest sissetungist alates. Oli võimalik valmistuda ka meediamajadel ja teistel teabevaldkonna olulistel organisatsioonidel. Sõjalise konflikti korral riigis, kus varasem sõjaaegne infohügieeni kogemus puudub, võib hüpoteesi kohaselt tsiviilelanike kohanemine uute sotsiaalmeediareeglitega oluliselt keerulisemalt kulgeda.

Seega võiks avalikkuse teavitamise peale rünnakuaegsest infohügieenist sotsiaalmeedias mõelda juba ennetavalt, näiteks osana Päästeameti kampaania „Ole valmis!“ tegevustest.

SOFIIA KOSTYTSKA

MTÜ Kriisiuuringute Keskus

E-post: sofiia.kostytska@kruk.ee

Sofiia Kostytska on Ukraina Kontrollikoja jurist ja MTÜ Kriisiuuringute Keskuse teadur, tema peamine uurimisvaldkond on rahvusvaheline õigus ning kriisijuhtimisega seotud õigus- ja finantsküsimused. Sofiia on omandanud 2018. aastal Kiievi Taras Ševtšenko Riiklikus Ülikoolis õigusteaduse magistrikraadi ning 2022. aastast omandab ta doktorikraadi Lvivi Äri- ja Õigusülikoolis.

HANNES NAGEL

MTÜ Kriisiuuringute Keskus

E-post: hannes.nagel@kruk.ee

Hannes Nagel on MTÜ Kriisiuuringute Keskuse asutajaliige ja juht, tema peamine uurimisvaldkond on kriisides otsustamine ja kriisijuhtimine. Hannes on omandanud 2021. aastal Tallinna Ülikoolis riigiteaduste magistrikraadi ning 2022. aastast omandab ta doktorikraadi Tallinna Ülikoolis, kus ta uurib adaptiivse valitsetuse strateegiad nüüdiskriiside ohjamisel.

ANNE-MAY NAGEL

MTÜ Kriisiuuringute Keskus

E-post: annemay.nagel@kruk.ee

Anne-May Nagel on MTÜ Kriisiuuringute Keskuse asutajaliige ja teadur, tema peamine uurimisvaldkond on kriisikommunikatsioon ja avaliku sektori säilenõtkus kriisides. Tal on 2018. aastast Tallinna Ülikoolis kommunikatsiooni magistrikraad. Ta töötab ka Tallinna Tehnikaülikoolis Ragnar Nurkse innovatsiooni ja valitsemise instituudi kommunikatsioonijuhina.

KASUTATUD ALLIKAD

[*Anon*.], 2008. Россия недооценивает информационный ресурс и проигрывает Западу [*Venemaa alahindab inforessurssi ja kaotab Läänele*]. *РИА 27 Регион,* 30. oktoober 2008. [Võrgumaterjal] Leitav: https://27r.ru/news/world/11817-2008-10-30-01-13-02 [Kasutatud 30.10.2022].

Aichner, T., Grünfelder, M., Maurer, O. & Jegeni, D., 2021. Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019. *Cyberpsychology, Behavior, and Social Networking*, 24(4), pp. 215–222.

Ajir, M. & Vailliant, B., 2018. Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, 12(3), pp. 70–89.

Al-Hlou, Y., Froliak, M., Hill, E., Browne, M. & Botti, D., 2022. Russian Troops Executed a Group of Ukrainian Men. *The New York Times*, May 21, 2022, 171(59369).

ArmyInform, 2022a. Як не стати поплічником ворога, інструкція для громадян [*Kuidas mitte saada vaenlase kaasosaliseks, juhised kodanikele*], 12. märts 2022. [Võrgumaterjal] Leitav: https://armyinform.com.ua/2022/03/12/infografika-yak-ne-staty-poplichnykom-voroga-instrukcziya-dlya-gromadyan [Kasutatud 30.10.2022].

ArmyInform, 2022b. *Список укриттів по всій Україні* [*Varjupaikade nimekiri* üle *Ukraina*]. 24. veebruar 2022. [Võrgumaterjal] Leitav: https://armyinform.com.ua/2022/02/24/spysok-ukryttiv-po-vsij-ukrayini [Kasutatud 30.10.2022].

ARTICLE 19, 1996. The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. *International Standards Series*, ARTICLE 19: London.

Barsukov, A. I., 1997. Приказы народного комиссара обороны СССР, 22 июня 1941 г.-1942 г. *[NSV Liidu Rahvakaitsekomissari käskkirjad, 22. juuni 1941–1942]*. Русский архив*:* Великая Отечественная, 13(2-2). Moskva: Terra.

Benedek, W., Bílková, V. & Sassòli, M., 2022. Report on Violations of International Humanitarian and Human Rights Law, War Crimes and Crimes against Humanity Committed in Ukraine since 24 February 2022. *OSCE*. [Võrgumaterjal] Leitav: https://www.osce.org/files/f/documents/f/a/515868.pdf [Kasutatud 30.10.2022].

Bilanishvili, G., 2021. *Security Review* on the New National Security Strategy of the Russian Federation. *Georgian Foundation for Strategic and International Studies*. [Võrgumaterjal] Leitav: https://gfsis.org.ge/files/library/pdf/English-3011.pdf [Kasutatud 15.08.2022].

Blank, S., 2014. Signs of New Russian Thinking About the Military and War. *Eurasia Daily Monitor*, 12(28). [Võrgumaterjal] Leitav: https://jamestown.org/program/signs-of-new-russian-thinking-about-the-military-and-war [Kasutatud 30.10.2022].

Bouwmeester, H., 2017. Lo and Behold: Let the Truth be Told – Russian Deception Warfare in Crimea and Ukraine and the Return of 'Maskirovka' and 'Reflexive Control Theory'. Rmt: P. A. L. Ducheine & F. P. B. Osinga, toim-d. *Netherlands Annual Review of Military Studies 2017: Winning Without Killing:The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*. T.M.C. Asser Press: Haag, pp. 125–153.

Bowen, G. A., 2009. Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, 9(2), pp. 27–40.

Broniatowski, D. A., Jamison, A. M., Qi, S., Al-Kulaib, L., Chen, T., Benton, A., Quinn, S. C., & Dredze, M., 2018. Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate. *American Journal of Public Health*, 108(10), pp. 1378–1384.

Brown, K., 2013. Agitprop in Soviet Russia. *Constructing the Past*, 14(1), pp. 5–8.

Chekinov, S. G. & Bogdanov, S. A., 2017. The Evolution of the Essence and Content of 'War' in the 21st Century. Военная Мысль, 1, pp. 43–45.

Cheong, M., & Lee, V. C. S., 2010. A microblogging-based approach to terrorism informatics: Exploration and chronicling sentiment and response to terrorism events via Twitter. *Information Systems Frontiers*, 13(1), pp. 45–59.

Choudhury, D. M., Monroy-Hernandez, A., & Mark, G., 2014. "Narco" emotions: affect and desensitization in social media during the Mexican drug war. *CHI '14: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 3563–3572. [Võrgumaterjal] Leitav: http://dx.doi.org/10.1145/2556288.2557197 [Kasutatud 30.10.2022].

Darczewska, J., 2014. The anatomy of Russian information warfare. The Crimean operation, a case study. *OSW Point of View*, 42. [Võrgumaterjal] Leitav: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf [Kasutatud 30.10.2022].

EIÕK, 2010. Inimõiguste ja põhivabaduste kaitse konventsioon, *Riigi Teataja*, RT II 2010, 14, 54, §10. [Võrgumaterjal] Leitav: https://www.riigiteataja.ee/akt/13320295 [Kasutatud 30.10.2022].

Euroopa Komisjon, 2018. A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation. Publications Office of the European Union: Luxembourg. [Võrgumaterjal] Leitav: https://

op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1 [Kasutatud 30.10.2022].

Giles, K. & Seaboyer, A., 2019. The Russian Information Warfare Construct. *Defence Research and Development Canada*. [Võrgumaterjal] Leitav: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf [Kasutatud 15.08.2022].

Glover, E., 2022. Kyiv's Retroville shopping centre unrecognisable following Russian airstrike. *The Independent*, March 22, 2022. [Võrgumaterjal] Leitav: https://www.independent.co.uk/news/world/europe/kyiv-retroville-russia-ukraine-airstrike-b2040897.html [Kasutatud 30.10.2022].

Grigas, A., 2016. *Beyond Crimea. The New Russian Empire.* New Haven; London: Yale University Press.

Herpen, van M. H., 2016. *Putin's Propaganda Machine – Soft Power and Russian Foreign Policy.* Lanham MA: Rowman & Littlefield.

Herzog, S., 2011. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, 4(2), pp. 49–60.

Hussain, A., 1994. Report of the Special Rapporteur on the Promotion and protection of the right to freedom of opinion and expression. *United Nations*, December 14, 1994, E/CN.4/1995/32. [Võrgumaterjal] Leitav: http://daccess-ods.un.org/access.nsf/Get?Open&DS=E/CN.4/1995/32&Lang=E [Kasutatud 30.10.2022].

IU, 2022a. Missile attack on TV tower near Rivne causes nine casualties, nine wounds – regional authorities. *Interfax-Ukraine*, March 14, 2022. [Võrgumaterjal] Leitav: https://en.interfax.com.ua/news/general/813288.html [Kasutatud 30.10.2022].

IU, 2022b. Vinnytsia's TV tower is under fire by occupiers, broadcasting temporarily turned off – service. Interfax-*Ukraine*, March 16, 2022. [Võrgumaterjal] Leitav: https://ua.interfax.com.ua/news/general/814161.html [Kasutatud 30.10.2022].

Kenez, P., 1986. The Birth of the Propaganda State: Soviet Methods of Mass Mobilization, 1917–1920. New York: Cambridge University Press.

Khan, I., 2021. Disinformation and freedom of opinion and expression. *United Nations*, A/HRC/47/25, April 13, 2021. [Võrgumaterjal] Leitav: https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/HRC/47/25&Lang=E [Kasutatud 30.10.2022].

Krepinevich, A., 2012. Cyber Warfare: A "Nuclear Option"? CSBA: Washington, DC.

Kvachkov, V., 2004. Спецназ России [*Venemaa eriväed*]. Военная Литература. [Võrgumaterjal] Leitav: http://militera.lib.ru/science/kvachkov_vv/index.html [Kasutatud 30.10.2022].

Law, J., 1993. *Organizing Modernity: Social Ordering and Social Theory.* Hoboken: Wiley-Blackwell.

Lotan, G., Graeff, E., Annany, M. & Gaffney, F. D., 2011. The Revolutions Were Tweeted: Information Flows During the 2011 Tunisian and Egyptian Revolutions. *International Journal of Communication*, 5, pp. 1375–1405.

Lukas, E. & Pomeranzev, P., 2016. Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. *Center for European Policy Analysis*. [Võrgumaterjal] Leitav: https://li.com/wp-content/uploads/2016/08/winning-the-information-war-full-report-pdf.pdf [Kasutatud 30.10.2022].

Manning, J., 2014. Social media, definition and classes of. Rmt: K. Harvey, toim. *Encyclopedia of social media and politics*. SAGE: Thousand Oaks, pp. 1158–1162.

McCauley, K. N., 2016. *Russian Influence Campaigns against the West: From the Cold War to Putin.* CreateSpace Independent Publishing Platform.

Merriam, S. B., 1988. *Case study research in education: A qualitative approach.* San Francisco: Jossey-Bass.

Murray, W., 2009. Military Adaptation in War. *Institute for Defense Analyses*. [Võrgumaterjal] Leitav: https://apps.dtic.mil/sti/pdfs/ADA509781.pdf [Kasutatud 30.10.2022].

Myers, S. L., 2022. Russians Use Bioweapon Lie To Smear U.S. *The New York Times*, September 5, 2022, 171(59537).

Oliker, O., 2022. Putin's Nuclear Bluff. *Foreign Affairs*, March 11, 2022. [Võrgumaterjal] Leitav: https://www.foreignaffairs.com/articles/ukraine/2022-03-11/putins-nuclear-bluff [Kasutatud 30.10.2022].

Panarin, I., 2008. Система информационного противоборства: механизм внешнеполитической пропаганды требует восстановления [*Teabekonfrontatsioonisüsteem: välispoliitiline propagandamehhanism tuleb taastada*]. *Военно-промышленный курьер*, 41(257).

Panchenko, O., 2022. What is not allowed to be published during the war. Important instruction. *The Village*, March 21, 2022. [Võrgumaterjal] Leitav: https://www.the-village.com.ua/village/city/instruction/324587-scho-ne-mozhna-publikuvati-pid-chas-viyni-vazhliva-instruktsiya [Kasutatud 30.10.2022].

Pipes, R., 1995. *A Concise History of the Russian Revolution.* New York: Vintage Books.

Prier, J., 2017. Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, 11(4), pp. 50–85.

Roblin, S., 2022. Ukrainian Forces Photobombed Russian sMercenaries – With Rockets. *Forbes*, August 15, 2022. [Võrgumaterjal] Leitav: https://www.forbes.com/sites/sebastienroblin/2022/08/15/ukrainian-forces-photobombed-russian-mercenaries-with-rockets/?sh=790b36f966a0 [Kasutatud 29.10.2022].

SBU, 2022a. Передавайте інформацію про окупантів, а не публікуйте дані про зсу чи результати ворожих обстрілів [*Edastage teavet okupantide osas, ent ärge avaldage andmeid tabamuste kohta*]. *Telegram*, 21. märts 2022. [Võrgumaterjal] Leitav: https://t.me/SBUkr/3959 [Kasutatud 31.10.2022].

SBU, 2022b. SSU detains blogger who published video of strike on Burshtyn TPP in Ivano-Frankivsk regiosn (video). *Ukraina Julgeolekuteenistus*, 20. oktoober 2022. [Võrgumaterjal] Leitav: https://ssu.gov.ua/en/novyny/sbu-zatrymala-blohera-yakyi-opryliudnyv-video-obstrilu-burshtynskoi-tes-na-ivanofrankivshchyni-video [Kasutatud 29.10.2022].

SBU, 2022c. Vinnytsia region: SSU detains four residents who filmed and shared videos with drone hit (video). *Ukraina Julgeolekuteenistus*, 19. oktoober 2022. [Võrgumaterjal] Leitav: https://ssu.gov.ua/en/novyny/na-vinnychchyni-sbu-zatrymala-4-meshkantsiv-yaki-znimaly-ta-peresylaly-video-z-prylotamy-video [Kasutatud 29.10.2022].

SBU, 2022d. SSU exposes russian special services on using smartphone games to recruit Ukrainian children (video). *Ukraina Julgeolekuteenistus*, 24. mai 2022. [Võrgumaterjal] Leitav: https://ssu.gov.ua/en/novyny/sbu-vykryla-spetssluzhby-rf-na-vykorystanni-smartfonihor-dlia-verbuvannia-ukrainskykh-ditei-video [Kasutatud 29.10.2022].

SBU, 2022e. *Як діяти військовослужбовцям у соцмережах* [*Kuidas sõjaväelased peaksid käituma sotsiaalsetes võrgustikes*]. *Ukraina Julgeolekuteenistus*. [Võrgumaterjal] Leitav: https://ssu.gov.ua/yak-diiaty-viiskovosluzhbovtsiam-u-sotsmerezhakh [Kasutatud 29.10.2022].

SBU, 2022f. Увага! Ворог створює фейкові чат-боти [*Tähelepanu! Vaenlane loob võltsitud vestlusroboteid*]. *Telegram*, 25. aprill 2022. [Võrgumaterjal] Leitav: https://t.me/dsszzi_official/3202 [Kasutatud 31.10.2022].

SBU, 2022g. *Захищаємо Україну разом*! [*Kaitske Ukrainat koos!*]. *Ukraina Julgeolekuteenistus*. [Võrgumaterjal] Leitav: https://ssu.gov.ua/zakhyshchaiemo-ukrainu-razom [Kasutatud 29.10.2022].

SKK, 2022. Увага зелені коридори до пекла [*Tähelepanu, rohelised koridorid põrgusse*]. *Telegram*, 26. mai 2022. [Võrgumaterjal] Leitav: https://t.me/CenterCounteringDisinformation/1669 [Kasutatud 31.10.2022].

SSSCIP, 2022. РЕПОСТ! [*JAGA!*]. *Ukraina Riiklik Side- ja Teabekaitseteenistus*, 15. märts 2022. [Võrgumaterjal] Leitav: https://t.me/dsszzi_official/2339 [Kasutatud 30.10.2022].

Stake, R. E., 1995. *The art of case study research.* Thousand Oaks, CA: Sage.

Stavridis, J. & Weinstein, D., 2017. Obama's Disclosure About Russian Hacking Is A Cybersecurity Gold Mine. *Huffington Post*, January 3, 2017. [Võrgumaterjal] Leitav: https://www.huffingtonpost.com/entry/the-disclosure-of-russias-hacking-is-a-goldmine-for-cybersecurity_us_5866b4cf4b0eb5864894ed6 [Kasutatud 30.10.2022].

Thomas, T. L., 2010. Russian Information Warfare Theory: The Consequences of August 2008. Rmt: S. Blank & R. Weitz, toim-d. *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*. Strategic Studies Institute: Carlisle, pp. 265–299.

Thomas, T. L., 2020. *The Chekinov-Bogdanov Commentaries of 2010–2017: What Did They Teach Us About Russia's New Way of War?* McLean: MITRE Corporation. [Võrgumaterjal] Leitav: https://apps.dtic.mil/sti/pdfs/AD1141587.pdf [Kasutatud 30.10.2022].

Ukraina Hääl, 2022. У «Дії» запустили збір коштів на допомогу армії через платформу UNITED24 [*„Diia" käivitas UNITED24 platvormi kaudu rahakogumise armee abistamiseks*], *Голос України*, 18. mai 2022. [Võrgumaterjal] Leitav: http://www.golos.com.ua/article/360210 [Kasutatud 31.10.2022].

Ukraina kultuuri- ja teabepoliitika ministeerium, 2021. Ключові завдання Центру [*Keskuse peamised ülesanded*], 6. jaanuar 2021. [Võrgumaterjal] Leitav: https://mkip.gov.ua/content/centr-strategichnih-komunikaciy-ta-informaciynoi-bezpeki-pri-ministerstvi-kulturi-ta-informaciynoi-politiki.html [Kasutatud 30.10.2022].

Ukraina kultuuri- ja teabepoliitika ministeerium, 2022. Що категорично заборонено публікувати під час війни [*Mida on sõja ajal rangelt keelatud avaldada*], 17. märts 2022. [Võrgumaterjal] Leitav: https://mkip.gov.ua/news/6971.html [Kasutatud 30.10.2022].

Ukraina valitsusportaal, 2022. *За підтримки Мінцифри запускають застосунок «Повітряна тривога» для оперативної реакції на початок і закінчення тривог* [*Digitaalarengu ministeeriumi toetusel käivitatakse rakendus* Õhuhäire*, et reageerida kiiresti häire algusele ja lõpule*], 1. märts 2022. [Võrgumaterjal] Leitav: https://www.kmu.gov.ua/news/za-pidtrimki-mincifri-zapushcheno-zastosunok-povitryana-trivoga-dlya-operativnoyi-reakciyi-na-pochatok-i-zakinchennya-trivog [Kasutatud 29.10.2022].

URJÜ, 2022. *Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану* [*Ukraina relvajõudude, teiste kaitseväeosade ja massiteabevahendite esindajate vahelise suhtluse korraldamise kohta sõjaseisukorra ajal*], №73, 3. märts 2022. [Võrgumaterjal] Leitav: https://www.mil.gov.ua/content/mou_orders/nakaz_73_zi_zminamu.pdf [Kasutatud 30.10.2022].

Van Assche, K., Beunen, R. & Duineveld, M., 2014. *Evolutionary Governance Theory.* Springer Cham.

Ülemraada, 2021. Про створення Центру протидії дезінформації [*Desinformatsioonivastase võitluse keskuse loomise kohta*], №106, 11. september 2021. [Võrgumaterjal] Leitav: https://zakon.rada.gov.ua/laws/show/n0015525-21#Text [Kasutatud 30.10.2022].

Ülemraada, 2022a. Про Заяву Верховної Ради України про цінність свободи слова, гарантії діяльності журналістів і засобів масової інформації під час дії воєнного стану [*Deklaratsioon sõnavabaduse tähtsuse, ajakirjanike ja meedia tegevuse tagatiste kohta sõjaseisukorra ajal*], №2190-IX, 14. aprill 2022. [Võrgumaterjal] Leitav: https://zakon.rada.gov.ua/laws/show/2190-20#n9 [Kasutatud 30.10.2022].

Ülemraada, 2022b. Кримінальний Кодекс України [*Ukraina kriminaalkoodeks*], 2341-III, №2198-IX, 23. märts 2022. [Võrgumaterjal] Leitav: https://zakon.rada.gov.ua/laws/show/2341-14#Text [Kasutatud 30.10.2022].

ÜRO, 1966. International Covenant on Civil and Political Rights. *Treaty Series*, 999.

Yates, C., & Partridge, H., 2015. Citizens and social media in times of natural disaster: Exploring information experience. *Information Research*, 20(1), pp. 1–24.

Weick, K. E., 2009. *Making Sense of the Organization: The Impermanent Organization*, 2nd edition. West Sussex: John Wiley & Sons Ltd.