Riigi Infosüsteemi Amet
Küberturvalisuse teenistus
Analüüsi- ja ennetusosakond

Venemaa sõda Ukrainas läbi küberdomeeni prisma

Vahekokkuvõte ja tähelepanekud

Märts 2022

24. veebruaril 2022 alustas Venemaa sõda Ukraina vastu. Füüsilise sõjategevuse kõrval toimub aktiivne mitmesuunaline tegevus ka küberruumis. Mõistagi ei kajastu kõik küberründed avalikes allikates. Kuna käesolev vahekokkuvõte põhineb suuresti avalikel allikatel, tasub lugemisel seda aspekti arvesse võtta.

Kokkuvõte:

- **Mis on sõja kontekstis küberruumis toimunud**?
  Suurem osa Ukraina suunal tehtud küberründeid pole olnud kriitilist infrastruktuuri halvavad. Rohkem on tehtud tehniliselt lihtsakoelisi küberründeid ja kasutatud saadud ligipääsusid nt infooperatsioonide läbiviimiseks, kuid on ka teada üksikud näited kriitilise infrastruktuuri mõjutamisest.
- **Kas ja kuhu jäi kübersõda?**
  Küberturvalisuse kogukondades ja laiemalt on Ukrainas toimuva sõja kontekstis arutletud selle üle, kas ja kuhu on jäänud ulatuslik sõda küberruumis. Teooriaid leidub mitmeid, näiteks:
  (1) küberründed on viis võimu näitamiseks mittekonventsionaalsel moel, kasutades ära nn halli ala, mis kaob, kui füüsiline sõda on käes;
  (2) küberrünne kriitilise infrastruktuurile võib kanduda üle teistesse riikidesse ja Venemaa pelgab seda, st ei taha (veel) eskaleerumist läänega;
  (3) Venemaa rakendab oma kübervõimekusi Ukraina ja lääneriikide vastu nn varuvariandina, kui sõjaline tegevus jookseb ummikusse ja sanktsioonide mõju on laastav.
- **Häktivistide ja kuritegelike rühmituste sekkumine**
  Mitmed rahvusvaheliselt tuntud kuritegelikud küberrühmitused ja häktivistid on seoses Ukraina sõjaga teatanud poole valimisest. Kui riiklike küberrühmituste kõrval aktiveeruvad poliitiliselt ka igasugused informaalsed kooslused, võib see küberruumi „haldamise" tulevikus keerulisemaks muuta. Nii tasub praegu küberruumis toimuvat tähelepanelikult jälgida, sest see annab aimu, mis aspektid tulevikus küberteemalistes aruteludes esile võivad kerkida.

Mis on sõja kontekstis küberruumis toimunud?

Küberründed Ukraina pihta ei saanud alguse koos sõjaga, vaid sealsed riigiasutused, kriitiline infrastruktuur ja muud teenused on küberrünnete sihtmärgiks olnud juba aastaid (nagu ka madalama aktiivsusega sõjategevus Ukrainas). Kui aga seada kitsamaid ajalisi raame, siis võiks öelda, et sõjalisele rünnakule hakati nähtavate ja pidevate küberrünnetega pinda laduma ja fooni looma tänavu aasta alguses.

<u>Näotustamine</u>

Selle aasta alguses muutusid küberründed avalikkusele nähtavamaks. Nimelt näotustati 13. jaanuaril kümnete Ukraina valitsusasutuste veebilehed ehk ründajad asendasid veebilehe sisu oma sõnumiga. Veebilehtedelt võis ukraina, vene ja poola keeles lugeda: „Ukrainlane! Kõik sinu isikuandmed on laetud avalikku võrku. Su arvutis olevad andmed on hävitatud, neid on võimatu taastada. Kogu teave sinu kohta on avalikuks tulnud, karda ja oota halvimat. See on sinu minevik, olevik ja tulevik."[1]

Ukraina valitsus kinnitas järgmisel päeval, et enamik mõjutatud veebilehti on taastatud ning isikuandmeid pole lekkinud ega muudetud. Veebilehtede näotustamine on tehniliselt suhteliselt lihtsakoeline küberrünne, kuid selle

kaudu edastatud sõnumite mõju võib olla suur: ärevuse tekitamine kodanikes, riigi autoriteedi õõnestamine, uurijate aja raiskamine *etc*.

Teenusetõkestusründed (DDoS)

Enne sõjategevuse algust tabasid jõulised teenusetõkestusründed Ukraina pankasid ja riigiasutuste veebilehti. Näiteks oli maas Ukraina riigile kuuluvate pankade (Privatbank ja Ošadbank) veebiteenused ning kaitseministeeriumi ja relvajõudude veebilehed. Pankade veebilehed olid küll kättesaadavad, ent näiteks kontole polnud võimalik sisse logida.

Ukraina küberpolitsei teatel saatsid ründajad pankade klientidele ka SMSe, milles teatati, et sularahaautomaadid ei tööta, kuid see polnud tõsi. Neid sõnumeid saadeti Eesti, Poola ja Austria numbritelt[2] [3]. Mitmed riigid, sh USA, Ühendkuningriigid[4], Austraalia ja ka Eesti[5], omistasid ründe Vene sõjaväeluurele (GRU). Venemaa saatkond USAs eitas süüd[6].

Päev enne Venemaa sõjalise rünnaku alustamist tabasid Ukraina valitsusasutusi ja pankasid samuti teenusetõkestusründed. See jätkus ka pärast sõjaseisukorra väljakuulutamist: maas on olnud Ukraina valitsusasutuste, julgeolekuteenistuse ja mitme ministeeriumi veebilehed.[7] Mitmed veebilehed on vahelduva eduga maas senini.

Hävitusvara

Ukraina infosüsteemidest ja võrkudest on alates tänavu aasta algusest leitud viite tüüpi hävituslikku pahavara. Tegu on andmete kustutamiseks ja seadmete kasutuskõlbmatuks muutmiseks mõeldud tööriistaga.

Esimene nendest oli jaanuaris ehk enne sõjalise pealtungi algust avastatud pahavara nimega **Whispergate**.[8] Oli teateid, et ühes Ukraina valitsusasutuses kustutas pahavara seitse tööjaama, teises asutuses nii tööjaamasid kui ka servereid.[9] Küberturvalisuse ettevõtte Cisco teatas[10] „mõõduka enesekindlusega", et pahavara paigaldanud häkkerid pääsesid valitsusasutuste süsteemidesse juba mitu kuud tagasi, ent aktiveerisid pahavara alles nüüd jaanuaris. Ukraina võimude sõnul oli neil tõendeid, et rünnaku taga on Venemaa ründajad.

Teine hävituslik pahavara – **HermeticWiper** – saadeti Ukraina suunal laiali vahetult enne Venemaa sissetungi Ukrainasse ehk 23. veebruaril. Küberturvalisuse ettevõtte ESET uurijate teatel[11] näitas pahavara ajatempel, et see loodi 28. detsembril 2021, mistõttu võiks arvata, et rünnet plaaniti juba siis. HermeticWiperi puhul väärib märkimist, et seda sama hävituslikku pahavara leidus ka Ukraina valitsusega koostööd tegeva ettevõtte Läti ja Leedu harukontorite võrgust.

Kolmas hävituslik pahavara – **IsaacWiper** – saadeti Ukraina riigiasutuse võrgu poole teele sissetungi päeval ehk 24. veebruaril.[12]

Väidetavalt sai ühega neist hävitusvaradest pihta ka Ukraina piiripunkt Rumeeniasse, mille tõttu pidi hakkama piiriületajaid vormistama paberi ja pliiatsi abil. Seda peetakse üheks põhjuseks, miks põgenike piiri ületamine nii kaua aega võttis.[13] [14]

Neljas Ukraina seadmetesse laiali saadetud hävituslik pahavara – **CaddyWiper** – avastati märtsis[15]. Küberturvalisuse ettevõtte ESET teatel kustutab pahavara kasutajaandmed ja vaheseinad kõigilt ketastelt, mis on kompromiteeritud seadmega seotud.

17. märtsil tuvastas CERT-UA õngitsuskampaania, mis püüab Ukraina ettevõtetesse süstida viiendat tüüpi hävitusvara, millele pandi nimeks **DoubleZero**.[16]

Nimetatud viis hävitusvara ei ole praeguse info kohaselt seni Eestisse jõudnud ja siinseid teenuseid või ettevõtteid puudutanud. Hävitusliku pahavaraga võivad seadmed nakatuda nii nagu ka iga teise pahavaraga (nt lunavara, nuhkvara). See tähendab, et oma süsteeme ja seadmeid saab hävitusvara eest kaitsta ka samamoodi, näiteks hoida

seadmed ja süsteemid uuendatud ning järgida küberhügieeninõudeid. Hävitusvaraga nakatumist aitab kõige lihtsamini üle elada eraldiseisvalt hoitud varukoopia.

Õngitsused

Microsofti teatel on häkkerite rühmitus Gamaredon (tuntud ka kui Actinium või Armageddon) Ukraina organisatsioone järjepidevalt õngitsuskirjadega sihtinud juba alates 2021. aasta oktoobrist. Ukraina valitsuse sõnul on rühmitus seotud Venemaa julgeolekuteenistuse FSBga. Rühmituse pahavaraga manustatud kirjade sihtmärkideks on olnud nii valitsusasutused, relvajõud, MTÜ-d, õiguskaitseorganid kui ka kohtud. Samuti on sihtmärkide seas organisatsioonid, mis Ukrainas rahvusvahelist või humanitaarabi pakuvad. Rünnete peamine eesmärk on olnud saada kätte tundlikku infot, säilitada ligipääs süsteemidele ja liikuda juba kompromiteeritud organisatsioonide kaudu järgmiste organisatsioonideni. Microsofti sõnul[17] koordineeritakse Gamaredoni küberluureoperatsioone Krimmist. Väidetavalt proovis rühmitus tänavu 19. jaanuaril kompromiteerida ka ühte Ukrainas tegutsevat Lääne organisatsiooni.[18]

Ent Gamaredon pole ainus, mis ukrainlaseid õngitsustega üle ujutab. Pärast Venemaa sõjalise rünnaku algust 24. veebruaril teavitas CERT-UA[19], et nende relvajõudude personali isiklike e-maili kontodele saadetakse massiliselt õngitsuskirju. Õngituskirjades palutakse saajal oma kontaktinfo verifitseerimiseks lingil klikkida, et nende kontot ei eemaldataks. Lingil klikkides aga seade nakatub. CERT-UA omistas selle õngitsuskampaania rühmitusele UNC1151 (tuntud ka kui Ghostwriter), mida on seostatud nii Valgevene kui ka Venemaaga.[20]

Sellele järgnesid hoiatused küberturvalisuse ettevõttelt Proofpoint[21], et on käimas õngitsuskampaania, milles kasutatakse Ukraina relvajõudude liikme kompromiteeritud e-maili (ukr@net), et sihtida Euroopa riikide ametnikke, kes tegelevad Ukraina sõjapõgenike logistikaga. Ühes uuritud õngitsuskirjadest oli peibutusteemaks NATO erakorraline kohtumine 23. veebruaril ja manuses pahavaraga fail. Ehkki küberturvalisuse ettevõte Proofpoint ei omistanud õngitsuskampaaniat veel ühelegi kindlale rühmitusele, tõdeti, et tõenäoliselt on tegemist riikliku taustaga ohustajaga.[22]

Lisaks on Amazoni teatel[23] pahavaraga manustatud õngitsuskirjade sihtmärgiks ka Ukrainas tegutsevad heategevuslikud organsatsioonid ja mittetulundusühingud. Ehkki konkreetseid organisatsioone ei nimetatud, olevat sihtmärkideks ravimite, toidu ja riietega varustamise üksused. Amazoni klientide seas on näiteks UNICEF ja Punane Rist.[24]

Õngitsuskirjadega sihitakse ka tavalisi Ukraina kodanikke, et nende kaudu infooperatsioone läbi viia või kellegi teise „kasulikuni" jõuda. Nimelt saatis CERT-UA välja eraldi hoiatuse[25], et nende kodanikele saadetakse õngitsuskirju kolme India organisatsiooni kompromiteeritud meiliaadresside kaudu.

Näiteks saadetakse kirju India autotööstuse ettevõtte TVS Rubber meiliaadressilt, kus kirja teemaks on pandud "*Увага*" ehk „tähelepanu". Õngitsuskiri suunab saaja lingile, kus teatatakse, et nende kontole on proovitud sisse logida Donetskis asuvalt IP-aadressilt ning seetõttu tuleb vahetada parooli. Kui inimene usub ja oma parooli sisestab, saavad ründajad tema kasutajaandmed kätte ning seega ligipääsu kontole. CERT-UA teatel on õngitsuste taga Venemaa eriteenistused, mis on varem need India organisatsioonid kompromiteerinud ning kasutavad neid nüüd ukrainlaste meiliaadressidele ligi pääsemiseks.[26] [27]

Infooperatsioonid

Osades küberrünnetes ei ole kesksel kohal veebilehe või teenuse töö häirimine, vaid selle sisu muutmine valeinfo või moonutatud info levitamiseks.

Ukraina võimude teatel on häkkerid pääsenud ligi mitme kohaliku omavalitsuse veebilehele, kus levitatakse valeinfot Kiievi langemise kohta ja väidetakse, et Moskvaga on sõlmitud rahuleping. Ukraina võimude teatel on häkkimise taga „vaenlane".[28] [29]

Lisaks levitasid häkkerid kompromiteeritud Ukraina uudistesaitidel (nt Ukraine 24) *deepfake* videot Ukraina presidendist Volodõmõr Zelenskist, kus ta kutsus ukrainlaseid üles relvi maha panema. Zelenski lükkas teate peatselt ümber. Võltsitud videot levitati uudistesaitidel, nt Ukraine 24 teatel[30] nende telekanalil ja veebisaidil, aga ka sotsiaalmeediaplatvormidel. Facebooki sõnul on nad video eemaldanud.[31] Võltsitud video kvaliteet oli võrdlemisi kehv, näiteks oli inimese nägu ja keha ebaloomulikult kokku pandud, samuti oli asend ning valgustus võlts. Ka Zelenski hääl oli tavapärasest madalam ja aeglasem.[32]

Rünnakud kriitilise infrastruktuuri pihta

Ukraina telekommunikatsiooniettevõte Triolan on saanud pihta küberrünnakutega, mis on põhjustanud internetikatkestusi mitmetes piirkondades. Väidetavalt on toimunud kaks rünnakut: üks 24. veebruaril ja teine 9. märtsil.[33] Rünnete tagajärjel lõpetasid mitu arvutit töö, sest ründajad lülitasid need ümber tehaseseadistustele.

Ettevõtte enda teatel häkiti sisse võrgu sõlmpunktidesse, millest umbes 70% (nt Kiievis, Harkivis, Odessas) on taastatud, kuid osasid ruutereid ei ole taastada õnnestunud. Ründest taastumine on raskendatud ka seetõttu, et osale varustusest peaks füüsiliselt ligi pääsema, kuid sõjategevuse tõttu oleks see töötajatele eluohtlik[34].

Internetikatkestusi üle riigi tekitab ka aktiivne sõjategevus, nt kommunikatsioonide pommitamine. Kahjustused infrastruktuurile on viinud rivist välja ka Ukrtelekomi pakutava internetiteenuse.[35]

Kas ja kuhu jäi kübersõda?

Alates Venemaa rünnakust Ukraina pihta on küberturvalisuse kogukondades ja laiemalt arutletud selle üle, kuhu on jäänud ulatuslik sõda küberruumis. Seni Ukraina suunal korraldatud teenusetõkestusründed ja näotustamised on pigem primitiivsed ründed – nendega ei vii riiki rivist välja ega alluta oma tahtele.

Näib, et eeldus laastavateks küberrünnakuteks sõjalise konflikti puhul oli üldiselt suurem. Näiteks 2015. aastal lõid häkkerid rivist välja Ukraina elektrivõrgu, mis viis tundideks majapidamistelt elektri[36]. Nüüd aga on kommunikatsioonid, haiglad ja muu kriitiline infrastruktuur küberrünnetest pigem puutumata jäänud. Rohkem on neid laastanud kuulirahe ja pommid.

Teooriaid, miks see nii on, leidub mitmeid. On arutletud[37], et küberrünnakud on rohkem võimu näitamiseks ning need põhjustavad kahju ilma konventsionaalsesse sõjategevusse astumata, kuna küberrünnakute puhul on otsest süüdlast tihti keeruline lõplikult välja selgitada. Need nii-öelda halli alasse jäämise eelised aga kaovad, kui füüsiline konflikt on juba käes.

Tuuakse ka välja, et pole põhjust arvata justkui Venemaal puuduksid ligipääsud ja võimekused Ukraina (või lääneriikide) kriitiliste üksuste ründamiseks.[38] Pigem võib Venemaa end selles osas veel lihtsalt tagasi hoida, et vältida eskaleerumist läänega, kuna küberründed võivad lihtsasti sihtmärgist kaugemale levida. Seda võis näha ka 2017. aastal Venemaa korraldatud[39] *NotPetya*-nimelise pahavararünnaku[40] puhul, mis oli mõeldud hävitama Ukraina ettevõtetes kasutatavat finantstarkvara. Ent pahavara kasutas levimiseks tuntud turvanõrkust, mistõttu valgus see laiali süsteemidesse üle maailma, hävitades andmeid ettevõtetes, näiteks suures Taani laevandusettevõttes Maersk[41].

Kuid üks üle Euroopa nähtavat mõju avaldanud küberintsident on sõjategevuse ajal siiski aset leidnud. Nimelt tabas ulatuslik küberrünne satelliitside pakkujat Viasati (täpsemalt nende KA-SAT satelliiti), mis jättis ühenduseta tuhanded inimesed üle Euroopa.[42] Intsident sai alguse 24. veebruaril ehk samal päeval, mil Venemaa ründas Ukrainat. Lisaks Ukrainale olid mõjutatud ka satelliitinterneti kasutajad näiteks Prantsusmaal, Saksamaal ja Poolas. Ründe olemust ja mõju uuritakse ning detaile – sealhulgas ründe võimalikku autorit – pole veel avaldatud.[43]

Teada aga on, et küberrünne KA-SAT satelliidi pihta lõi muuhulgas rivist välja ka 5800 tuulegeneraatori töö Kesk-Euroopas. Tuulikud kuuluvad Saksamaa energiaettevõttele Enercon, mille teatel oli häiritud tuulegeneraatorite kaugmonitoorimine ja –kontrollimine.[44]

Nii enne sõja algust kui ka sõja ajal on läänemeelsete riikide ametid (nt EE, UK, USA, CAN) jaganud hoiatusi kriitilise infrastruktuuri üksustele kõrgendatud küberohu tõttu ning soovitanud üle vaadata oma küberturvalisuse olukord ja võtta kasutusele täiendavaid meetmeid. Ohu taset on tõstnud nii see, et Ukraina üksuste pihta tehtud rünnakute mõju võib ulatuda ka teistesse riikidesse, kui ka see, et Venemaa võib võtta küberruumis eraldi sihtmärgiks riigid, mis on Ukrainale häälekalt poolehoidu avaldanud ja Venemaale ranged sanktsioonid kehtestanud.[45]

Sealjuures on ka pakutud[46], et Venemaa hoiab oma agressiivseid küberrelvi veel nii-öelda reservis, et need kasutusele võtta siis, kui sõjategevus jõuab ummikusse ja sanktsioonid valusalt pitsitavad. Sel juhul võivad ka ründajad tavapärasest riskialtimad olla, kuivõrd Venemaa on muust maailmast juba suhteliselt ära lõigatud ega pea rahvusvahelise reaktsiooni ja sanktsioonide hirmus end sedavõrd piirama.

Samas tasub aga rõhutada, et kõik NATO liikmed on kinnitanud, et ka küberrünnak võib vajadusel viia NATO artikkel 5 käivitamiseni.[47]

Praeguses faasis ei pruugi ulatuslikud küberründed lääneriikide pihta Venemaale ka otsest geopoliitilist kasu tuua. Pigem oleks neil hoopis lääneriike ja Ukrainat ühendav mõju. Samas tegutseb Venemaa hoogsalt küberruumi nn halli ala piires, kasutades küberründeid lisaks luureinfo kogumisele infooperatsioonideks ja teenuste häirimiseks, et vähendada inimeste moraali ja usku Ukraina (või mõne teise riigi) võimekusse. Lisaks lastakse vabalt vohada sealsel kübervandalismil ja –kuritegevusel, kuniks nende sihtmärgid Venemaa oponentide omadega kattuvad.

Häktivistide ja kuritegelike rühmituste sekkumine

Mõistagi tegutsevad riiklike sidemetega küberrühmitused oma riiklike huvide vaimus. Mõneti märkimisväärsem on aga see, et seoses sõjaga Ukrainas, on ka mitmed rahvusvaheliselt tuntud kuritegelikud küberrühmitused ja häktivistid teatanud poole valimisest. Näiteks teatas Venemaal tegutsev Conti lunavararühmitus, et toetab täielikult Venemaa presidenti Vladimir Putinit ning ähvardas rünnata Kremli vaenlaseid, kui need peaksid Venemaa tegevusse sekkuma.[48] Näib aga, et kõik rühmituse liikmed pole sama meelt, sest üks väidetavalt Ukraina juurtega rühmituse liige lekitas pahameele väljendamiseks rühmituse sisemised vestlused.[49]

Conti lunavararühmitus kogus mullu kurikuulsust sellega, et ründas lirimaa tervishoiusüsteemi. Krüpteeritud süsteemide tõttu oli takistatud juurdepääs diagnostikale ja meditsiinilistele dokumentidele. Lisaks varastasid ja avalikustasid ründajad patsientide tundlikke andmeid. Süsteemi täielikuks taastamiseks läks aega mitu kuud.[50]

Ehkki Conti lubas praeguse sõja kontekstis Venemaa vaenlaseid rünnata, siis infot nende korraldatud rünnakute kohta lääne asutuste ja ettevõtete vastu seni napib.

Vastukaaluks on aktiivse ja nii-öelda ukrainameelse rolli võtnud häktivistide rühmitus Anonymous (ja sellega mestis olevad grupid). Rühmitus on teatanud paljudest rünnetest Venemaa riigiasutuste ja teiste organisatsioonide pihta. Näiteks on võetud maha veebilehti ja teenuseid, varastatud hulgaliselt andmeid ja muudetud andmekogude, kaustade ja failide nimesid ukrainameelseks (nt *Slava Ukraini, „putin stop this war"*)[51]. Mõned konkreetsed teated rünnetest:

- Anonymouse teatel ründasid nad Venemaa kaitseministeeriumit ja lekitasid info selle töötajate kohta;
- mitmed Venemaa riigiasutuste ja teiste organisatsioonide veebilehed on alates sõja algusest pidevalt maas olnud;
- Anonymouse teatel ründasid nad korduvalt Vene riiklikke telekanaleid, kus pandi mängima Ukraina hümn ja muusika ning näidati videokaadreid Venemaa sõjalisest hävitustööst Ukrainas;
- Anonymous teatas, et nad pääsesid ligi Venemaa avalikele kaameratele. Väidetavalt võeti üle rohkem kui 400 avalikku kaamerat, mille videopilti jagati rühmituse enda loodud veebilehel. Kaamerad jaotati kategooriate järgi: näiteks ärid, õuekaamerad, restoranid, koolid, kontorid jne;
- Anonymous teatas, et rünnati Venemaa Tuumainstituuti, kust varastati ja lekitati väidetavalt 40 000 dokumenti. Rühmitus kutsus inimesi üles tõlkega abistama;[52]

- Anonymouse teatel pääsesid nad ligi Roskomnadzori süsteemidele, kust varastasid ja lekitasid 360 000 faili. See on agentuur, mis kontrollib, haldab ja tsenseerib meediat riigis.[53]

Poole valimisest on teatanud ka mitmed teised ideoloogiliselt motiveeritud küberrühmitused, mida võrreldes Conti ja Anonymousega võib pidada pigem vähetuntuks. Oluline on aga märkida, et rühmituste **väidetesse toime pandud rünnete kohta tasub suhtuda ettevaatlikult**, sest paljudele neist puudub sõltumatu kinnitus või tõestus. Nii võivad osad väited küberrünnakutest olla osa infooperatsioonidest või lähtuda muudest rühmituse omakasupüüdlikest motiividest.

Väiteid teenusetõkestusrünnetest (DDoS) on võimalik lihtsamini kontrollida, sest veebilehe või teenuse töötamist/mittetöötamist saab kergesti tuvastada. Keerulisem lugu on aga väidetega, kus teatatakse rünnetest tähtsate organsatsioonide pihta ning nende andmete varastamisest ja lekitamisest. CheckPointi teatel näitas nende tehtud analüüs, et paljud taolistest väidetest ei ole tõesed, kuna kuvatõmmised ja andmed väidetavalt varastatud infost on tegelikult lekkinud juba varem, info on aegunud või lihtsalt madala väärtusega.[54]

Näiteks teatas Anonymous, et on rünnanud ja rivist välja löönud Venemaa kosmoseagentuuri Roskosmose süsteemid. Väidetavalt puuduvat seetõttu Venemaal ligipääs oma luuresatelliitidele. Lisaks väideti, et kustutati konfidentsiaalseid andmeid, mis seotud kosmoseagentuuri satelliitfotodega ja sõidukite monitoorimissüsteemiga. Neid väiteid pole õnnestunud kontrollida. Roskosmose sõnul on tegemist valeinfoga ja nende süsteemid töötavat tavapäraselt. Kusjuures Roskosmose juht sõnas, et riigi satelliitide ründamist tõlgendataks kui sõja alustamist.

Kommentaar, et rünnet satelliitide pihta tõlgendataks kui sõjakuulutust, toob aga päevakorda olulise mõttekoha häktivistide (ja teiste eraviisiliste häkkerite) sekkumise osas sõjategevusse ja/või ka laiemalt poliitikasse. Teoreetiliselt: kui näiteks häktivistid ründaksid Venemaa satelliite ja seda tõlgendataks kui sõja alustamist, siis kellele riik sõja kuulutaks? Kas rühmitusele? Riigile, mille pinnal rühmitus tegeleb? Või midagi kolmandat?

Muidugi on need küsimused osalt utreeritud, kuid siiski võib siin näha sugemeid teemadest ja küsimustest, mis kübervaldkonnas aset leidvates kõnelustes võivad edaspidi rohkem tooni andma hakata.

Küberit võib üldiselt pidada pigem ähmaseks domeeniks. On keeruline ja osadel juhtudel ka võimatu ajada jälgi, kes või mis on mõne küberrünnaku taga. Viimastel aastatel on tehtud rahvusvaheliselt palju ponnistusi (sh Eesti eestvedamisel) selleks, et küberruum ei oleks piltlikult öeldes metsik lääs, kus reeglid ja õigus ei kehti. Nii on paljud riigid üle maailma rõhutanud, et rahvusvaheline õigus kehtib ka küberruumis, kokku leppinud vastutustundliku käitumise printsiibid küberruumis (sh Venemaa) ning loonud võimalused selle rikkujate vastutusele võtmiseks. Rünnete omistamine ja ründajate sanktsioneerimine saavad aina enam juurutatud. Samas on nende meetmete fookuses pigem riigid ja nendega otseselt seotud küberrühmitused.

Kui aga poliitiliselt aktiveeruvad ka igasugused informaalsed kooslused häkkeritest, mis ei ole seotud otseselt ühegi riigiga, siis muudab see küberruumi „haldamise" keerulisemaks. Taolised grupeeringud ei pruugi lasta end häirida riigi poliitilistest ja diplomaatilistest raamidest, kuivõrd selle liikmed võivad olla paljudest riikidest üle maailma. Selliselt on keeruline rühmituse tegevust ka ühegi konkreetse riigiga siduda ning suureneb ka oht, et rünnaku süüdlasena mängitakse välja riik, mis seda tegelikult ei ole. Seega tasub taolistel arengutel silma peal hoida, sest need võivad tulevikus hakata suurel määral mõjutama küberteemade arutelusid ja protsesse nii rahvusvahelisel areenil kui ka siseriiklikult.

---

[1] https://therecord.media/hackers-deface-ukrainian-government-websites/

[2] https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/

[3] https://cip.gov.ua/en/news/shodo-kiberataki-na-saiti-viiskovikh-struktur-ta-derzhavnikh-bankiv

[4] https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine

[5] https://vm.ee/et/uudised/eesti-uhineb-ukraina-vastaste-kuberrunnakute-omistamise-avaldustega

[6] https://www.reuters.com/world/russia-rejects-claims-it-was-responsible-cyberattack-ukraine-2022-02-19/
[7] https://www.reuters.com/world/europe/ukrainian-government-foreign-ministry-parliament-websites-down-2022-02-23/
[8] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
[9] https://zetter.substack.com/p/hackers-were-in-ukraine-systems-months?s=r
[10] https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html
[11] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
[12] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
[13] https://venturebeat.com/2022/02/27/ukraine-border-control-hit-with-wiper-cyberattack-slowing-refugee-crossing/
[14] https://www.washingtonpost.com/world/2022/02/26/europe-welcomes-refugees-ukraine-russia/
[15] https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/
[16] https://cert.gov.ua/article/38088
[17] https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
[18] https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/
[19]https://www.facebook.com/UACERT/posts/pfbid0s4MvRCVkpdXvoD4SvfUPDKJc4239MXYXYd1aAHazyinTUuKxENhcXp4yr7mTxE3El
[20] https://www.bleepingcomputer.com/news/security/ukraine-links-belarusian-hackers-to-phishing-targeting-its-military/
[21] https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails
[22] https://thehackernews.com/2022/03/hackers-try-to-hack-european-officials.html
[23] https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine
[24] https://www.bleepingcomputer.com/news/security/amazon-charities-aid-orgs-in-ukraine-attacked-with-malware/
[25] https://m.facebook.com/UACERT/posts/3174820937443897rdr
[26] https://thehackernews.com/2022/03/ukrainian-cert-warns-citizens-of.html
[27] https://securityaffairs.co/wordpress/128789/cyber-warfare-2/cert-ua-warns-phishing-ukrainian-citizens.html
[28] https://www.reuters.com./world/europe/ukrainians-say-hackers-used-local-government-sites-spread-fake-capitulation-news-2022-03-03/
[29] https://www.bleepingcomputer.com/news/security/ukraine-says-local-govt-sites-hacked-to-push-fake-capitulation-news/
[30] https://www.facebook.com/www.ukraine24.ua/posts/1847515155441880
[31] https://twitter.com/ngleicher/status/1504186935291506693
[32] https://www.forbes.com/sites/zacharysmith/2022/03/16/hacked-ukrainian-tv-station-transmits-fake-zelensky-surrender-announcement/
[33] https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/
[34] https://therecord.media/ukraines-internet-infrastructure-struggles-as-russian-invasion-continues/
[35] https://ukrtelecom.ua/presscenter/5-bereznya-2022/
[36] https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)
[37] https://www.nature.com/articles/d41586-022-00753-9
[38] https://thecyberwire.com/stories/75ca5313b59045ccbcbfc7d3b9e5d207/ukraine-russia-will-not-waste-offensive-cyber-weapons
[39] https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack
[40] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[41] https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack

[42] https://www.datacenterdynamics.com/en/news/viasats-ka-sat-network-still-disrupted-by-suspected-cyberattack-more-than-two-weeks-later/

[43] https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/

[44] https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/

[45] https://www.lawfareblog.com/cyber-realism-time-war

[46] https://thecyberwire.com/stories/75ca5313b59045ccbcbfc7d3b9e5d207/ukraine-russia-will-not-waste-offensive-cyber-weapons

[47] https://www.nato.int/cps/en/natohq/news_185000.htm

[48] https://www.cpomagazine.com/cyber-security/as-ukraine-war-rages-conti-ransomware-gang-throws-support-behind-russian-government/

[49] https://www.cpomagazine.com/cyber-security/after-declaring-support-for-russian-invasion-conti-ransomware-gang-hit-with-data-leak/

[50] https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

[51] https://www.websiteplanet.com/blog/cyberwarfare-ukraine-anonymous/

[52] https://securityaffairs.co/wordpress/128527/hacktivism/anonymous-hit-russian-nuclear-institute.html

[53] https://www.infosecurity-magazine.com/news/anonymous-leaked-files-russian/

[54] https://blog.checkpoint.com/2022/03/03/hacktivism-in-the-russia-ukraine-war-questionable-claims-and-credits-war/