VENEMAA JÄTKAB KÜBERRUUMIS NÕRGA LÜLI OTSIMIST

Küberrünnetega püüab Venemaa Ukrainas toetada oma üldisi eesmärke: murda ukrainlaste vastupanu, õõnestada valitsuse mainet ning häirida riigi toimimist. Küberluure on tõenäoliselt suurim küberruumist tulenev oht.

Venemaa alahindas Ukraina küberruumi vastupidavust ning Lääne ja küberturvalisuse ettevõtete abi.

Jätkuvad ähvardavad postitused sotsiaalmeedias ja küberründed osana mõjutustegevusest Ukrainat aktiivselt toetavate riikide, sh Eesti vastu.

Juba vähemalt alates Ukraina–Venemaa sõja algusest, 2014. aastast, on Ukraina olnud Venemaa eriteenistuste küberrünnete alaline sihtmärk.[1] Need intensiivistusid vahetult enne kineetilise sõjategevuse algust ning jätkusid kineetilise sõjapidamise aktiivse faasi jooksul. Peamiselt korraldas Venemaa küberründeid osana mõjutustegevusest, näiteks teenustõkestus- ja näotustamisründeid, andmelekkeid. Sellise tegevuse üks eesmärke on takistada riigil jagamast infot oma kodanikega, tekitada neis hirmu ja usaldamatust riigi juhtkonna vastu, nõrgestada ühiskonnas vastupanu ning luua infomüra, et tegelikkuse eristamine väärinfost oleks keeruline. Pärast kineetilise sõjapidamise aktiivsemat faasi püüdis Venemaa hoida Ukraina riiki nõrgana ning korraldas kriitilisi teenuseid häirivaid küberründeid.[2] Madalama aktiivsusega küberründeid, peamiselt luure eesmärgil, korraldati seni, kuni Venemaa oma Ukraina-suunalist retoorikat taas agressiivsemaks muutis. 2022. aasta jaanuaris ja veebruaris sooritati Ukraina vastu küberründeid, millega Venemaa püüdis tõenäoliselt toetada oma üldisi eesmärke: murda Ukraina ühiskonna vastupanu, tekitades ka küberrünnetega mulje Venemaa suurest ülekaalust ja olukorra lootusetusest Ukraina jaoks ning Ukraina riigi nõrkusest.

13.01.–14.01.2022 murdsid küberründajad Ukraina riigiasutuste veebilehtedele ja muutsid need avalikkusele kättesaamatuks. Samal ajavahemikul levitasid küberründajad Ukraina arvutivõrkudes pahavara WhisperKill/WhisperGate.[3]

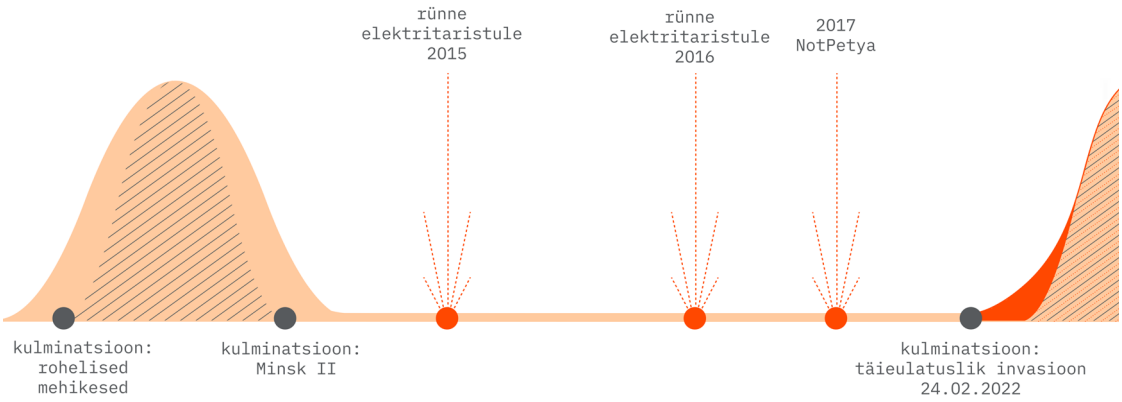
15.02.–16.02.2022 toimusid teenustõkestusründed Ukraina riigiasutuste ja pankade veebilehtedele.[4]

1 Vähemalt alates 2014. aastast on FSB 18. keskus juhendanud küberründeid Ukraina vastu, sh info varastamiseks, https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy.

2 2015. ja 2016. aastate detsembris korraldas GRU Ukraina energiasektorile küberründed, mis tõid kaasa paaritunnised elektrikatkestused Lääne-Ukrainas. 2017. aastal korraldas GRU nn NotPetya küberoperatsiooni, millega küberründajad püüdsid Ukraina valitsusasutuste andmed kasutuskõlbmatuks muuta. https://www.wired.com/story/sandworm-kremlin-most-dangerous-hackers

3 https://cert.gov.ua/article/18101; https://ssu.gov.ua/en/novyny/sbu-rozsliduie-prychetnist-rosiiskykh-spetssluzhb-do-sohodnishnoi-kiberataky-na-orhany-derzhavnoi-vlady-ukrainy; https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion; 27.04.2022, Microsoft, Special Report: Ukraine An overview of Russia's cyberattack activity in Ukraine.

4 27.04.2022, Microsoft, Special Report: Ukraine An overview of Russia's cyberattack activity in Ukraine.



Mõni tund enne kineetilise sõjategevuse taasaktiveerumist sagenesid Ukraina-vastased küberründed järsult veelgi.

> 23.02.2022 toimusid teenustõkestusründed Ukraina valitsusasutuste ja pankade veebilehtedele.
>
> 23.02.–25.02.2022 paigaldasid küberründajad Ukraina infosüsteemidesse mitut erinevat pahavara, mis on võimelised häirima arvuti kasutamist, muutma arvutid kasutuskõlbmatuks või tegema kättesaamatuks arvutis olevad andmed. Näiteks 23.02.2022 paigaldas GRU Ukraina valitsusasutuste, IT, energia- ja finantssektori infosüsteemidesse hävitusvara HermeticWiper ning korraldas 24.02.22 küberründe Viasati tütarettevõttele KA-SAT, paigaldades viimase infosüsteemi hävitusvara AcidRain.[5]

Kui Lääs eristab küberründeid ja mõjutustegevust rangemalt, siis lihtsustatult öeldes käsitab Venemaa neid ühe kontseptsioonina – informatsiooniline vastasseis (*информационное противоборство*). See Venemaa Relvajõudude doktriin koosneb kolmest põhikomponendist: teise riigi mõjutamine informatsioonilis-tehniliselt ja -psühholoogiliselt ning Venemaa enda kaitsmine selliste mõjutuste eest.

Võimalik, et esialgu ei korraldatud energia, veevarustuse või muu sarnase kriitilise taristu spetsiifilisi küberründeid,[6] mis tooksid kaasa teenuse pikaajalisi katkestusi, kuna Venemaa eeldas et ta saavutab sõjalised eesmärgid kiiremini ning tal oli kasumlikum hoida kohalike elanike soosingut.

Hoolimata esialgse kavatsuse luhtumisest, hõivata Ukraina alad paari päevaga, jätkas Venemaa küberrünnetega Ukraina vastu. On märgata perioode, kus need on sagedasemad. Näiteks märtsi teisest poolest kuni ligikaudu kuu jooksul tuvastasid Ukraina küberkaitsjad koos küberturvalisuse ettevõtetega korduvalt hävituslikku pahavara.

5 https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-oneurope/
6 Rünnak tööstuskontrolli spetsiifilistele infosüsteemidele, mida kasutavad elutähtsatest teenustest näiteks energia- ja vee-ettevõtted, on mõnevõrra erinev tavaliste infosüsteemide ründamisest. Lihtsustatult öeldes on nende infosüsteemid erinevalt üles ehitatud. Pahavara Industroyer2 on arendatud tööstuskontrolli spetsiifilisi infosüsteeme ründama, seda kasutas tõenäoliselt GRU 08.04.2022 Ukraina energiasektori ründamisel. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Ning sügisest hakkasid küberründed taas hoogu koguma.[7] Seejuures on jätkunud küberründed teabehanke eesmärgil.[8] Küberluure on tõenäoliselt kõige suurem oht, mis tuleneb küberruumist. Varastatud infot on näiteks võimalik efektiivselt kasutada sisendina Vene relvajõudude operatsioonideks või mõjutustegevuseks.

> Sõja vältel on Venemaa kasutanud mitut hävitusvara korduvalt. 11.10.22 tuvastas Microsoft hävitusvara CaddyWiper Mõkolajivi ja Kiievi regiooni kriitilisest taristust. Esimest korda tuvastas küberturvalisuse ettevõte ESET seda hävitusvara 14.03.22 Ukraina panga infosüsteemist.[9]
>
> 14.10.22 tuvastas Microsoft Ukraina ja Poola logistika- ja transpordiettevõtete infosüsteemis lunavara Prestige.

2022. aastal on küberturvalisuse uurijad tuvastanud Ukraina küberruumis vähemalt üheksa pahavara (hävitusvara), millega on püütud teenuseid häirida (ENISA Threat Landscape 2022, lk 25; Recorded Future, 2022[10]). Hävitusvara on pahavara tüüp, mis lihtsustatult öeldes muudab arvuti kasutuskõlbmatuks, rikkudes programme või andmeid. Selle saavutamiseks võib kasutada näiteks ka lunavara, mis krüpteerib andmed, ilma võimaluseta neid dekrüpteerida (nt lunavara Prestige). Nii palju hävitusvara nii lühikese aja vältel ei ole varem kusagil esinenud. See näitab, et Venemaa on suuteline lühikese ajaga arendama uusi pahavarasid.

Tõenäoliselt on Venemaa küberrünnete eesmärk sarnaselt relvajõudude tegevusele kurnata Ukraina küberkaitsjaid ning leida seejärel nõrgim lüli, mis aitaks kaasa Venemaa üldise sõjalise eesmärgini jõudmisele – kurnata Ukrainat, kahjustada Ukraina juhtkonna rahvusvahelist mainet ja usaldust, vähendada liitlaste abi ning õõnestada ühiskonna moraali. Selleks ei olegi nii oluline iga küberründega tegelikult häirida infosüsteemi, sest iga ründe korral tuleb uurijatel kulutada inim- ja ajaressurssi kontrollimaks, kas infosüsteemi on rünnatud, kui ulatuslikult ning kuidas parandada kaitset jmt.

Venemaa alahindas Ukraina küberruumi vastupidavust ning Lääne ja küberturvalisuse ettevõtete abi Ukrainale. Hoolimata teenustõkestusrünnetest riigiasutuste veebilehtedele, et takistada mh info edastamist, on Ukraina valitsus leidnud alternatiivseid suhtlusviise, näiteks kasutanud sotsiaalmeediat. Oluline roll tsiviil- ja militaarsektoris side hoidmisel on ka Starlinki seadmete kasutamisel. Alates 2014. aastast pakuvad küberturvalisuse ettevõtted Ukrainale abi oma küberruumi kaitsmisel. Abi intensiivistus Venemaa täieulatusliku invasiooni ajal ning koostöös liitlaste toega on see tõenäoliselt osutunud määravaks Ukraina küberruumi kerksusel. Oodatud mõju ei ole avaldanud ka Venemaa mõjutustegevus küberruumis. Ukraina ühiskond püsib ühtsena ja usaldab oma valitsust, hoolimata ähvardavatest postitustest sotsiaalmeedias ja andmeleketest.

Venemaa küberründed ulatuvad ka väljapoole Ukraina territooriumi. Ukrainat toetavate riikide, sh Eesti, Läti, Leedu ja Poola küberruumi ohustavad Kremli-meelsed küberründajad. Nad on kineetilise sõja aktiivses faasis püüdnud hirmutada ühiskondi ähvardavate postitustega sotsiaalmeedias, teenustõkestusrünnete ja andmeleketega. Nende tegevus toetab Venemaa eriteenistuste mõjutustegevust.

7 Tuvastatud küberrünnakutest vt nt https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/
8 https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/
9 https://twitter.com/ESETresearch/status/1503436420886712321
10 https://go.recordedfuture.com/hubfs/reports/mtp-2022-0512.pdf

116.08.–17.08.2022 toimusid teenustõkestusründed Eesti ettevõtete ja riigiasutuste infosüsteemidele.[11] Vene-meelsed häktivistid võtsid need küberründed omaks ning väitsid, et on rünnanud Eesti suunal 207 sihtmärki.[12] Tegelikult kajastati pelgalt nimekirja, kus on võimalik Smart-ID teenuseid kasutada ning kõigi nende vastu ründeid ei sooritatud.

Venemaa püüab küberrünnetega toetada oma strateegilisi eesmärke, sh tekitada hirmu ja nõrgestada ühiskonna vastupanu agressoriga võitlemiseks; häirida riigi toimimist; luua infomüra, et tegelikkuse eristamine väärinfost oleks keeruline; õõnestada kodanike usaldust riigi juhtkonda. Ukraina–Venemaa sõda kinnitab, et küberturbe meetmeid rakendades[13] on võimalik vastu pidada nii küberluure, -sabotaaži kui ka mõjutustegevuse rünnete vastu.

Ründevahend	Eesmärk	Kaitsemeede
näotustamisründed	• hirmutamine / ähvardamine • segaduse külvamine	Veebilehe tarkvara uuendamine. Veebilehte teiselt ettevõttelt tellides veendu ka tema hoolsuses rakendada küberturvalisuse meetmeid. Näotustamisel kasuta võimalusel alternatiivseid infokanaleid, nt sotsiaalmeediat. Peamised sihtmärgid: meedia, riigiasutused (kriisi info vahendajad), veebilehti pakkuvad ettevõtted
teenustõkestusründed	• info liikumise takistamine • hirmutamine	Teenustõkestusrünnete kaitse (vt RIA soovitusi)[14]
sotsiaalmeedia postitused	• hirmutamine / ähvardamine	Kontrolli väiteid usaldusväärsetest allikatest ja ole allikakriitiline. Lisaks vt nõuandeid infosõja käitumise kohta veebilehelt kriis.ee
andmeleke	• maine kahjustamine (vähendada liitlaste abi, luureinfo jagamist)	Mõtle hoolikalt läbi, millist infot ja kellega jagad. Veendu, et Sinu jagatud infot hoitakse turvaliselt, et info saaja hoiab jagatud infot keskkonnas, kus on rakendatud küberturvalisuse parimat praktikat
andmeid krüpteeriv pahavara	• riigi toimimise häirimine • hirmutamine	Varunda andmeid korrektselt
arvuteid hävitav pahavara	• riigi toimimise häirimine • hirmutamine	Hoia tarkvara uuendatuna. Rakenda küberturvalisuse parimat praktikat. Varunda andmeid korrektselt
küberluure (õngitsemine, jõurünne, turvanõrkuste kasutamine)	• info kogumine • varastatud info lekitamine kontekstist välja rebitult, koos fabritseeritud infoga	Hoia tarkvara uuendatuna. Rakenda küberturvalisuse parimat praktikat. Osale küberhügieeni koolituste

11 https://www.ria.ee/uudised/16-ja-17-augusti-ummistusrunnakute-sihtmarke-oli-paarkummend
12 https://www.runews24.ru/society/17/08/2022/a66e4f36646d32e3bb459604947b3390?
13 Vaata küberturvalisuse meetmete soovitusi RIA veebilehelt https://www.ria.ee
14 https://www.ria.ee/kuberturbe-nouanded/nouanded-asutusele-ja-ettevottele/teenusetokestusrunde-ennetus