



Küberkuritegevus rahvusvahelises kriminaalõiguses

Nr 9

12.06.2024

Küberrünnakud rahvusvaheliste kuritegudena

Küberrünnakud on arvutisüsteemide vastu ja nende abil toime pandud kuriteod.¹ Kuigi paljudes riikides võivad riigisisese õiguse kohaselt olla küberrünnakud kriminaalkorras karistatavad, ei ole neid seni reguleeritud rahvusvaheliste kuritegudena Rahvusvahelise Kriminaalkohtu (edaspidi RKK) Rooma statuudis.²

Küberrünnakutega on näiteks võimalik digitaalse teabe abil infosüsteeme häirida, nendesse sekkuda eesmärgiga süsteem välja lülitada, selles rikkeid esile kutsuda, selle tõhusust vähendada jne. Teisalt on võimalik ka süsteemi korruptsioon ehk süsteemi andmete ja algoritmide volituseta muutmine, takistades süsteemi nõuetekohast toimimist. Seejuures võib korruptsiooni mõju tuvastamine olla sageli keeruline, mistõttu võib ka probleemi kiire lahendamine olla suur väljakutse. Samuti on võimalik küberrünnakute abil toimivaid süsteeme hävitada.³

Lisaks süsteemidele kujutavad küberrünnakud märkimisväärset ohtu inimõigustele, demokraatiale ning üldisele rahvusvahelisele rahule ja stabiilsusele.⁴ Tehnoloogia ja digimaailma arenguga kaasneb ka paljude kuritegude jõudmine võrgukeskkonda. Selliselt on võimalik veebi teel panna toime pettuseid, kuid ka raskemaid kuritegusid nagu terrorism, inimkaubandus jne.⁵ Kuna võrgukeskkond võimaldab kurjategijatel viibida füüsiliselt mujal, mitte sündmuskohal, on teatud kuritegude rahvusvaheline toimepanemine lihtsustatud.⁶

Küberkuritegevuse kriminaliseerimine rahvusvahelises karistusõiguses

Rooma Statuudi artikli 5¹ kohaselt kuuluvad RKK jurisdiktsiooni genotsiid, inimsusevastased kuriteod, sõjakuriteod ja agressioonikuriteod.⁷ Küberrünnakud ei paigutu ühegi eelnimetatud kuriteo alla. Tulenevalt küberrünnakute ähvardavast ohust rahvusvahelisele julgeolekule ja inimkonnale, on siiski vajalik kaaluda nende rahvusvahelist kriminaliseerimist. Seda enam, et

¹ Why and how is the Council of Europe working against cybercrime? – Cybercrime. Council of Europe Portal. – <https://www.coe.int/en/web/cybercrime> (27.11.2023).

² Rome Statute of the International Criminal Court. Rome: UN General Assembly 1998.

³ Libicki, M. C. Cyberspace in peace and war. Maryland: Naval Institute Press 2016, p. 19-20.

⁴ Why and how is the Council of Europe working against cybercrime? – Cybercrime. Council of Europe Portal. – <https://www.coe.int/en/web/cybercrime> (27.11.2023).

⁵ Cybercrime. – Migration and Home Affairs. European Commission. – https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en (27.11.2023).

⁶ Brush, K., Rosencrance, L., Cobb, M. Cybercrime. (09.2021) – Threats and Vulnerabilities. TechTarget. – <https://www.techtarget.com/searchsecurity/definition/cybercrime> (28.11.2023).

⁷ Rome Statute of the International Criminal Court. Rome: UN General Assembly 1998.

RKK ise on hiljuti sattunud küberrünnaku ohvriks.⁸ Ka RKK peaprokurör Karim A. A. Khan on seisukohal, et küberrünnakud võivad potentsiaalselt täita mitmete juba määratletud rahvusvaheliste kuritegude põhiomadusi, mistõttu tuleks need ka kriminaliseerida.⁹

Rahvusvahelise Kriminaalkohtu jurisdiktsiooni piirangud

Oluliseks piiranguks küberrünnakute rahvusvahelisel kriminaliseerimisel võib osutuda Rooma statuudi artikli 22 lõikes 2 sätestatud *nullum crimen sine lege* põhimõte, mille kohaselt tuleb kuriteo määratlust tõlgendada rangelt ja seda ei tohi laiendada analoogia alusel. Seega puudub RKK-l sisuliselt pädevus küberkuritegevuse vastu süüdistuse esitamiseks, kuivõrd neid ei ole selgelt statuudis määratletud.¹⁰

Seejuures võib küberrünnakuid hüpoteetiliselt kvalifitseerida ka juba reguleeritud rahvusvaheliste kuritegude alla. Ennekoike võiks küberrünnakute kasutamist sõjalises tegevuses pidada sõjakuriteoks. Näiteks on Venemaa Föderatsiooni relvajõudude kindralstaabi peavalitsus (GRU) pannud sõja ajal toime küberrünnakuid mitmete Ida-Ukraina valitsusasutustesse ja ettevõtetesse tungimiseks. Rünnakute ohvriteks langesid paljud, sh meediakanalid, raudteefirmad ja haiglad. Tagajärjeks on olnud ulatuslikud elektrikatkestused ja vähemalt kolme piirkondliku teenuseettevõtte sulgemine. Seega võiks relvakonfliktis küberoperatsioonide läbiviimist potentsiaalselt pidada sõjakuriteoks. Eriti, kui tegemist on tsiviilisikute sihipärase ründamisega või selgelt ebaproportsionaalse tsiviilkahju tekitamisega.¹¹ Kui küberrünnakuid kasutatakse näiteks agressiooni või inimsusevastase kuriteole omaste tagajärgede saavutamiseks, saaks neid ka vastavate kuritegude alla kvalifitseerida.¹² Niisamuti võib kübertegevust kasutada genotsiidi õhutamiseks või tuumakahjustuse algatamiseks, et tappa massiliselt teise rahvusliku grupi liikmeid.¹³

Teine potentsiaalne piirang võib tuleneda statuudi artiklist 17, mille kohaselt peab juhtum olema piisavalt tõsine, et õiguskaitseasutus saaks sellele reageerida. Seda piirangut ei ole aga keeruline ületada, kuivõrd küberoperatsioonid, mis põhjustavad elu kaotamist või tõsist kahju füüsilisele varale, on ilmselgelt piisavalt tõsised.¹⁴

Kolmandaks võib piiravaks osutuda ka küberoperatsioonide omistamine konkreetsele riigile. See võib kujutada endast üsna suurt väljakutset, sest riigid võivad varjata oma osalust, tegutsedes mitteriiklike osapoolte kaudu. Seetõttu on küberoperatsioonide eest vastutavate konkreetsete isikute kindlakstegemine ja vastutusele võtmine keeruline. Lisaks võib kohtu jurisdiktsioon rahvusvaheliste kuritegude toimepanemist võimaldavate küberoperatsioonide üle eeldada operatsiooni toimumist mõne osalisriigi territooriumil või läbiviimist mõne osalisriigi kodaniku poolt. See tähendab, et kohtul ei pruugi olla siiski pädevust olukorras, kus küberrünnakute mõju esineb kolmanda riigi territooriumil.¹⁵

⁸ Measures taken following the unprecedented cyber-attack on the ICC. – International Criminal Court. <https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc>

⁹ Yoon Onn, K. C. The Prosecutor's New Policy on 'Cyber Operations' before the International Criminal Court (and its Implications for Ukraine): Some Preliminary Reflections. (15.09.2023) – EJIL: Talk! Blog of the Journal of International Law. <https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-the-international-criminal-court-and-its-implications-for-ukraine-some-preliminary-reflections/> Khan KC, K. A. A. Technology Will Not Exceed Our Humanity. – Digital Front Lines. <https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/>

¹⁰ Sterio, M., Trahan, J. Cyber Operations As Crimes At The International Criminal Court. Articles of War. <https://lieber.westpoint.edu/cyber-operations-crimes-icc/>

¹¹ Tharan, J. The Criminalization of Cyber-operations Under the Rome Statute. – Journal of International Criminal Justice 2021/19 (5). p. 1155.

¹² Ibid., p. 1158.

¹³ Tharan 2021, p. 1160.

¹⁴ Sterio, M., Trahan, J. Cyber Operations As Crimes At The International Criminal Court. – Articles of War. <https://lieber.westpoint.edu/cyber-operations-crimes-icc/>

¹⁵ Ibid.

Rahvusvaheline küberturvalisus

Eelnevalt kirjeldatud piirangute ületamiseks on oluline rahvusvaheline koostöö. Peamine aspekt siinkohal on küberturvalisus, mis on leidnud rakendust nii riigisisestes kui ka rahvusvahelises õiguses. Üldiselt määratletakse küberturvalisust meetmetena arvuti või arvutisüsteemi kaitseks volitamata juurdepääsu või rünnaku eest.¹⁶

Rahvusvaheline koostöö toimub nii õiguslikult kui ka mitte-õiguslikult siduvate tööde või aktide kaudu.¹⁷ Seega, kuigi küberrünnakud ei pruugi veel rahvusvahelises õiguses kriminaliseeritud olla, on siiski erinevaid lepinguid ja juhiseid, mis nende vastu kaitse tagavad. Seejuures on mõned olulisemad küberturvalisuse organisatsioonid Euroopa Liit, Euroopa Nõukogu, NATO, ÜRO ja OECD.¹⁸

Rahvusvahelise õiguse kehtivust küberkuritegevuse valdkonnas ilmestab näiteks Tallinna Manuaal¹⁹, mis sisaldab põhjalikku analüüsi sellest, kuidas olemasolev rahvusvaheline õigus kohaldub küberkonfliktides, rõhutab küberrünnakute omistamise keerukust ja nõuab õiguslike raamistike täpsustamist. Seega on tegemist mõjuka allikaga nii juristidele kui ka poliitikutele, kes tegelevad küberteemaliste küsimustega.²⁰

Üks olulisemaid õiguslikult siduvaid lepinguid on Budapesti konventsioon ehk arvutikuritegevusvastane konventsioon.²¹ Konventsiooni artikli 23 kohaselt teevad osalisriigid tihedat koostööd arvutisüsteemide ja -andmetega seotud kuritegude uurimiseks ja menetlemiseks ning kuritegude elektrooniliste tõendite kogumiseks, järgides peatükis „rahvusvaheline koostöö” sätestatud, kriminaalasjades tehtavat rahvusvahelist koostööd käsitlevaid rahvusvahelisi ning ühtsete õigusaktide alusel sõlmitud kokkuleppeid ja oma riigi õigusakte.²²

Viimaks on juba aastaid arutletud rahvusvahelise küberruumi kriminaalkohtu loomise vajaduse üle. Kohtu pädevuses oleks karistada isikuid, kes on toime pannud tõsisid rahvusvahelisi küberkurtegeid.²³ Selleks oleks ka jurisdiktsiooni sätteid hõlmav ülemaailmne leping hädavajalik, reguleerimaks kõige tõsisemad ning ülemaailmset julgeolekut ohustavad küberkuriteod.²⁴ Niisiis, kuivõrd RKK-l puudub sisuliselt pädevus selliste kuritegude eest isikuid vastutusele võtta, võiks lahenduseks olla eraldiseisva kohtu moodustamine.

Kokkuvõte

Küberkuritegevuse kriminaliseerimine rahvusvaheliselt on igal juhul vajalik. Küberoperatsioonid ja -rünnakud kannavad üha enam sõjalisi eesmärke ning muutuvad rahvusvaheliste kuritegude toimepanemise vahendiks. Kuigi olemasolev küberjulgeolek võib olla tõhus kaitsevahend, on siiski oluline edendada rahvusvahelist koostööd lepingute, suuniste ja ühiste jõupingutuste kaudu

¹⁶ Hitchens, T., Goren, N. International Cybersecurity Information Sharing Agreements. – Centre For International & Security Studies At Maryland. <https://cissm.umd.edu/sites/default/files/2019-07/Cyber%20information%20sharing%20agreement%20report%20-%20102017%20-%20FINAL.pdf> p. 4.

¹⁷ Tharan 2021, p. 1139.

¹⁸ Tiirmaa-Klaar, H. Rahvusvaheline koostöö küberjulgeoleku tagamisel. – Diplomaatia. 2010/85, p. 6-7.

¹⁹ The Tallinn Manual. – Research. The NATO Cooperative Cyber Defence Centre of Excellence. <https://ccdcoc.org/research/tallinn-manual/>

²⁰ Ibid.

²¹ Convention on Cybercrime. Budapest: Council of Europe 2001.

²² Arvutikuritegevusvastane konventsioon. – RT II 2003, 9, 32.

²³ Schjolberg, S. Draft United Nations Treaty on an International Criminal. 10th Ed. (06.2015) – Court or Tribunal for Cyberspace. – https://www.cybercrimelaw.net/documents/Draft_Treaty_text_on_International_Criminal_Tribunal_for_Cyberspace.pdf (29.11.2023). Art 1.

²⁴ Schjolberg, J. Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes. (03.2012) – EastWest Institute Cybercrime Legal Working Group. <https://www.cybercrimelaw.net/documents/ICTC.pdf> (29.11.2023), p. 9-10.

küberkaitse tugevdamiseks ülemaailmsel tasandil. Nii on ka rahvusvahelise küberruumi kriminaalkohtu loomine oluline samm globaalselt kasvava küberkuritegude toimepanemise vastu.

Laureen Hansmer
praktikant
õigus- ja analüüsiosakond

Kasutatud allikad

1. Arvutikuritegevusvastane konventsioon. – RT II 2003, 9, 32.
2. Brush, K., Rosencrance, L., Cobb, M. Cybercrime. (09.2021) – Threats and Vulnerabilities. TechTarget. – <https://www.techtarget.com/searchsecurity/definition/cybercrime>.
3. Convention on Cybercrime. Budapest: Council of Europe 2001.
4. Cybercrime. – Migration and Home Affairs. European Commission. – https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en
5. Hitchens, T., Goren, N. International Cybersecurity Information Sharing Agreements. (20.10.2017) – Centre For International & Security Studies At Maryland. <https://cissm.umd.edu/sites/default/files/2019-07/Cyber%20information%20sharing%20agreement%20report%20-%20102017%20-%20FINAL.pdf>
6. Libicki, M. C. Cyberspace in peace and war. Maryland: Naval Institute Press 2016.
7. Measures taken following the unprecedented cyber-attack on the ICC.– International Criminal Court. <https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc>
8. Rome Statute of the International Criminal Court. Rome: UN General Assembly 1998.
9. Schjolberg, S. Draft United Nations Treaty on an International Criminal. 10th Ed. (06.2015) – Court or Tribunal for Cyberspace. – https://www.cybercrimelaw.net/documents/Draft_Treaty_text_on_International_Criminal_Tribunal_for_Cyberspace.pdf
10. Schjolberg, J. Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes. (03.2012) – EastWest Institute Cybercrime Legal Working Group. <https://www.cybercrimelaw.net/documents/ICTC.pdf>
11. Sterio, M., Trahan, J. Cyber Operations As Crimes At The International Criminal Court– Articles of War. <https://lieber.westpoint.edu/cyber-operations-crimes-icc/>
12. Tharan, J. The Criminalization of Cyber-operations Under the Rome Statute. – Journal of International Criminal Justice 2021/19 (5).
13. The Tallinn Manual. – Research. The NATO Cooperative Cyber Defence Centre of Excellence. <https://ccdcoe.org/research/tallinn-manual/>
14. Tiirmaa-Klaar, H. Rahvusvaheline koostöö küberjulgeoleku tagamisel. – Diplomaatia. 2010/85.
15. Why and how is the Council of Europe working against cybercrime? – Cybercrime. Council of Europe Portal. – <https://www.coe.int/en/web/cybercrime>.
16. Yoon Onn, K. C. The Prosecutor's New Policy on 'Cyber Operations' before the International Criminal Court (and its Implications for Ukraine): Some Preliminary Reflections. (15.09.2023) – EJIL: Talk! Blog of the Journal of International Law. <https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-the-international-criminal-court-and-its-implications-for-ukraine-some-preliminary-reflections/> (27.11.2023); Khan KC, K. A. A. Technology Will Not Exceed Our Humanity. – Digital Front Lines. <https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/>