https://doi.org/10.22364/juzk.83.50

VALSTU STARPTAUTISKĀ ATBILDĪBA KIBERTELPĀ PAR KIBEROPERĀCIJĀM

INTERNATIONAL RESPONSIBILITY OF STATES IN CYBERSPACE FOR CYBER OPERATIONS

Sabīne Stirniņa, ***Mg. iur.***

Summary

In an era where the digital environment permeates almost every aspect of modern life, the traditional concept of sovereignty faces a formidable opponent – cyber operations. The landscape of global power dynamics has changed irreversibly, with cyber operations becoming a powerful tool to interfere in the sovereign prerogatives of states. This threat is further exacerbated by the availability and affordability of the technology needed to launch cyber operations. The dynamic development of cyberspace raises questions about its interaction with the typically conservative system of state responsibility. Therefore, the author of this article examines the legal dimensions of cyberspace, assessing possible violations of state sovereignty and exploring the problems of attributing cyber operations to states.

Atslēgvārdi: kiberoperācijas, valstu atbildība, kibertelpa, suverenitāte

Keywords: cyber operations, state responsibility, cyberspace, sovereignty

Ievads

Mūsdienu automatizētajā un digitalizētajā pasaulē masveida iznīcināšanas potenciāls vairs nav tikai valstu rīcībā – arī nevalstiski dalībnieki un organizācijas spēj rīkot kiberoperācijas, kas apdraud ekonomiku, cilvēktiesības un valsts drošību. Valstis, organizācijas un uzņēmumi ir kļuvuši atkarīgi no informācijas tehnoloģiju infrastruktūras, kas nodrošina kritisko pakalpojumu un sistēmu darbību, – sākot no elektrotīkliem, kodolenerģijas un resursu ieguves līdz militārajai aizsardzībai un veselības aprūpei. Līdz ar to kibertelpa ir kļuvusi par jaunu arēnu konfliktiem, kurā iespējams darboties, apejot teritoriālo robežu ierobežojumus. Šajā kontekstā pastāv daudz neatrisinātu jautājumu, taču rakstā vispirms tiks analizēta suverenitātes loma valstu kiberdarbību regulēšanā, jo tieši kibertelpas teritoriālā rakstura trūkums rada izaicinājumus tās piemērošanai, bet pēc tam – kiberoperāciju attiecināšanas problemātika.

1. Starptautiski prettiesiskas rīcības izpausme kibertelpā

Kibertelpas pirmsākumos tiesību zinātnieki apšaubīja iespēju tai piemērot pastāvošo suverenitātes principu, tā vietā iestājoties par īpaša tiesiska regulējuma

izstrādi. Deivids R. Džonsons (*David R. Johnson*) un Deivids Posts (*David Post*) uzsvēra, ka, "atdaloties no doktrīnas, kas saistīta ar teritoriālo jurisdikciju, radīsies jauni noteikumi, lai regulētu daudzas jaunas parādības, kurām nav skaidra paralēle nevirtuālajā pasaulē"[1]. Tomēr šī pieeja ir mainījusies. Piemēram, 2024. gada nogalē Eiropas Savienības Padome apstiprināja ES un tās dalībvalstu deklarāciju par kopīgu izpratni par starptautisko tiesību piemērošanu kibertelpā. Deklarācijā uzsvērts, ka kibertelpai ir piemērojami vairāki starptautisko tiesību pamatprincipi, tostarp valsts suverenitāte, neiejaukšanās princips, spēka lietošanas aizliegums, kā arī starptautisko humanitāro tiesību, cilvēktiesību un valstu atbildības tiesību ievērošana.[2]

Šajā kontekstā neskaidrība rodas no divu atšķirīgu uzskatu pastāvēšanas. Viena pieeja apšauba, vai suverenitāte ir patstāvīgs starptautisko tiesību princips, savukārt otra to uzskata par juridiski īstenojamu starptautisko tiesību normu.

1.1. Suverenitāte – noteikums vai princips?

Saskaņā ar "suverenitātes kā noteikuma" pieeju suverenitāte darbojas kā starptautisko tiesību norma, kuru var pārkāpt. Jau 1861. gadā Henrijs Halleks (*Henry Halleck*) apgalvoja, ka teritoriālās varas ekskluzivitāte ir suverēnas valsts "ideālās tiesības" un "neatkarīgi no tā, ko viena valsts var pieprasīt kā savas ideālās tiesības, ikvienas citas valsts absolūts pienākums ir tās atzīt. Atteikt to, lai arī ar kādu ieganstu, būtu starptautiskās jurisprudences pozitīvās normas un pamatprincipa pārkāpums"[3]. Savukārt attiecībā uz kibertelpu Tallinas rokasgrāmata 2.0 (*Tallinn Manual 2.0*) paredz, ka valstis nedrīkst veikt kiberoperācijas, kas pārkāpj citu valstu suverenitāti.[4] Kopš Tallinas rokasgrāmatas 2.0 publicēšanas suverenitātes kā noteikuma koncepcija ir guvusi ievērojamu atsaucību – valstis, kā, piemēram, Irāna, Jaunzēlande un Nīderlande, šādu skatpunktu ir atbalstījušas savās pozīcijās par starptautisko tiesību piemērošanu aktivitātēm kibertelpā.[5]

Turpretim "suverenitātes kā principa" piekritēji uzskata, ka suverenitāti nevar pārkāpt, jo tā nedarbojas kā patstāvīga starptautisko tiesību norma.[6] Lai kiberoperāciju varētu uzskatīt par starptautisko tiesību pārkāpumu, tai būtu jāpārkāpj spēka lietošanas aizlieguma vai iejaukšanās aizlieguma princips. Uz šādu pieeju norāda vien pāris valstis. Apvienotās Karalistes bijušais augstākais tieslietu padomnieks Džeremijs Raits (*Jeremy Wright*) ir norādījis, ka "nevar ekstrapolēt konkrētu noteikumu vai papildu aizliegumu attiecībā uz kiberdarbībām, izņemot aizliegtu iejaukšanos; tāpēc

---

[1] Johnson D. R., Post D. Law and Borders – The Rise of Law in Cyberspace. Stanford Law Review, Vol. 48, 1996, p. 1376.

[2] Council of the European Union. Declaration of a Common Understanding of International Law in Cyberspace, 15833/24, 2024, p. 3.

[3] Halleck H. International Law: Or, Rules Regulating the Intercourse of States in Peace and War. San Francisco: H. H. Bancroft, 1861, p. 272.

[4] Schmitt M. N. (gen. ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyberoperations. Cambridge University Press, 2017, p. 17.

[5] Iran. Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, 2020, para. 4; New Zealand. The Application of International Law to State Activity In Cyberspace, 2020, p. 2; Government of the Netherlands. Letter to the parliament on the international legal order in cyberspace. Appendix I: International law in cyberspace, 2019, p. 2.

[6] Corn G., Taylor R. Sovereignty in the Age of Cyber. AJIL Unbound, Vol. 111, 2017, p. 210.

Apvienotās Karalistes valdības nostāja ir tāda, ka pašreizējās starptautiskajās tiesībās šādu noteikumu nav"[7]. Autore uzskata, ka šāda pieeja paplašina pieļaujamo ļaunprātīgo darbību tvērumu kibertelpā. Piemēram, nesankcionēta iejaukšanās kiberinfrastruktūrā pati par sevi netiktu uzskatīta par suverenitātes pārkāpumu. Tāpat arī kiberoperācijas, kā, piemēram, iefiltrēšanās un datu iegūšana no valdības vai privātajiem tīkliem, visticamāk, nekvalificētos kā starptautisko tiesību pārkāpumi, ja suverenitāti traktētu kā vispārīgu principu, nevis saistošu tiesību normu.

Tomēr jānorāda, ka salīdzinoši nesen ANO Starptautiskā tiesa apstiprināja, ka suverenitāte ir primārs noteikums. Tiesa izskatīja Kostarikas prasību pret Nikaragvu par teritoriālās suverenitātes un spēka lietošanas aizlieguma pārkāpumu, jo Nikaragva bez piekrišanas izmantoja savu armiju, lai padziļinātu upi Kostarikas teritorijā. Rezultātā tiesa atzina, ka Nikaragvas rīcība pārkāpusi Kostarikas teritoriālo suverenitāti, un tādējādi neuzskatīja par vajadzīgu izskatīt Kostarikas prasību par spēka izmantošanu.[8] Uz to, ka suverenitāti var uzskatīt par noteikumu, īpaši norāda tiesas vārdu izvēle, proti, vārds "pārkāpusi". Turklāt jāuzsver, ka visas tiesvedības laikā puses neapstrīdēja, ka pastāv visaptveroša norma, kas aizliedz suverenitātes pārkāpumu. Gluži pretēji, puses savus argumentus balstīja tieši uz šo normu. Līdz ar to vienprātība starp iesaistītajām pusēm par šāda noteikuma pastāvēšanu nodrošināja pamatu, uz kuru tiesa balstīja spriedumu, apstiprinot tā būtisko nozīmi starptautiskajās tiesībās.

1.2. Kritēriji suverenitātes pārkāpuma noteikšanai

Lai gan nav iespējams precīzi noteikt robežu, no kuras kiberoperācija kļūst par citas valsts suverenitātes pārkāpumu, pastāv dažādas pieejas šī jautājuma interpretācijai. Starptautiskā ekspertu grupa, kas piedalījās Tallinas rokasgrāmatas 2.0 izstrādē, kiberoperāciju tiesiskumu vērtēja no diviem aspektiem – cietušās valsts teritoriālās integritātes aizskāruma pakāpi un to, vai ir notikusi valdības funkciju uzurpācija.[9]

Pirmkārt, lielākā daļa ekspertu bija vienisprātis, ka kiberoperācija, kas rada fizisku kaitējumu citas valsts teritorijā, nepārprotami pārkāpj tās teritoriālo suverenitāti. Papildus fiziskam kaitējumam citā valstī izvietotas kiberinfrastruktūras funkcionalitātes zuduma izraisīšana var būt suverenitātes pārkāpums, lai gan nav nosakāms precīzs slieksnis, jo pašlaik nav izteikta *opinio juris*. Tika panākta pilnīga vienprātība par to, ka kiberoperācija, kas izraisa funkcionalitātes zudumu, ciktāl kiberinfrastruktūrai nepieciešams remonts vai nomaiņa, ir uzskatāma par teritoriālās suverenitātes pārkāpumu. Piemēram, "Shamoon" vīruss, kura dēļ 2012. gadā bija jāmaina tūkstošiem Saūda Arābijas naftas uzņēmuma "Saudi Aramco" cietos diskus, tiktu kvalificēts kā suverenitātes pārkāpums.[10]

Otrkārt, eksperti secināja, ka kiberoperācija, kas iejaucas citas valsts valdības funkciju veikšanā, ir suverenitātes pārkāpums. Lai gan viņi nesniedza precīzu "valdības

[7] Wright J. Speech: Cyber and International Law in the 21st Century, 2018. Pieejams: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [aplūkots 20.03.2025.]

[8] ANO Starptautiskās tiesas 16.12.2015. spriedums lietā "Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)", Judgment, 2015 ICJ 665, para. 66.

[9] Schmitt M. N., 2017, p. 20.

[10] Ibid., pp. 20–21.

funkciju" definīciju, pastāvēja vienprātība, ka jebkura kiberoperācija, kas traucē būtisku valdības funkciju veikšanai nepieciešamo datu vai pakalpojumu pieejamību, pārkāpj suverenitāti. Piemēram, tas attiecas uz datu dzēšanu vai manipulāciju, kas var apdraudēt sociālo pakalpojumu sniegšanu, vēlēšanu norisi, nodokļu iekasēšanu, diplomātisku darbību efektivitāti un valsts aizsardzības pasākumu īstenošanu.[11]

Tallinas rokasgrāmatas 2.0 suverenitātes pārkāpuma testu lielā mērā ir ietekmējusi "uz sekām balstīta pieeja" jeb "efektu doktrīna" (*effects doctrine*). Lai gan pašlaik nav skaidrs, kāda ir valstu nostāja par "uz sekām balstīto" pieeju suverenitātes pārkāpumiem kibertelpā, pastāv norādes, ka vairākas valstis apsver šādas pieejas pieņemšanu. Piemēram, Francijas valdība savā 2019. gada paziņojumā norādīja, ka jebkādas sekas, ko ar kiberlīdzekļiem rada uzbrukumi Francijas teritorijā, var tikt uzskatītas par suverenitātes pārkāpumu.[12] Dažas valstis ir ierosinājušas, ka suverenitātes pārkāpumu novērtējumā jāņem vērā ne tikai kiberuzbrukumu intensitāte, bet arī to ietekme uz sabiedrību.[13] Čehija ir identificējusi vairākas situācijas, kas var tikt uzskatītas par suverenitātes pārkāpumu, piemēram, kiberuzbrukumus, kas izraisa cilvēku nāvi, infrastruktūras traucējumus vai apdraud datu pakalpojumus, kuri ir būtiski valdības funkciju veikšanai, piemēram, izspiedējprogrammatūras uzbrukums, kas kavē pensiju izmaksu.[14] Savukārt Jaunzēlande uzskata, ka ne katra nesankcionēta iejaukšanās kibertelpā ir suverenitātes pārkāpums.[15] Tomēr valdošā izpratne liecina, ka suverenitāte tiek pārkāpta, ja kiberoperācija izraisa vismaz nevēlamas sekas vai efektus citā valstī.

Attiecīgi valsts teritoriālās integritātes un suverenitātes aizskārums ir neapstrīdams, ja kiberoperācija ietekmē kritisko infrastruktūru vai kiberinfrastruktūru, izraisot fizisku kaitējumu vai funkcionalitātes zudumu. Tomēr šauras pieejas piemērošana šī jautājuma izvērtēšanā nav pamatota, jo fiziskas sekas ne vienmēr materializēsies. Ja teritoriālās suverenitātes pārkāpuma konstatēšanu balstītu vien uz materiālu kaitējumu vai sistēmu darbības traucējumiem, tādas darbības kā nesankcionēta piekļuve datorsistēmām un informācijas drošības kompromitēšana nepārsniegtu suverenitātes pārkāpuma slieksni.

Turpretim pārmērīgi plaša suverenitātes interpretācija, kurā jebkura ārvalsts kiberdarbība automātiski tiktu uzskatīta par suverenitātes pārkāpumu neatkarīgi no tās ietekmes uz cietušās valsts infrastruktūru, ir vienlīdz problemātiska. Šāda pieeja ignorētu starptautisko mijiedarbību tiešsaistē un varētu radīt nesamērīgas tiesiskās sekas. Līdz ar to ir nepieciešams līdzsvarots risinājums, kas vienlaikus ņemtu vērā gan kiberdrošības apdraudējumu nopietnību, gan starptautisko tiesību principus un mijiedarbību starp valstīm.

Tā vietā, lai koncentrētos uz kiberoperāciju fiziskajām sekām, autori iesaka pievērst uzmanību kiberoperāciju tehniskajiem pamatiem, fokusējoties uz datorsistēmas vai kiberinfrastruktūras integritāti. Tehniskā kritērija izvirzīšana par prioritāti

---

[11] Schmitt M. N. 2017, pp. 21–22.

[12] Ministère des Armées. Droit international appliqué aux opérations dans le cyberespace, 2019, pp. 6–7.

[13] Moynihan H. The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention. Chatham House: The Royal Institute of International Affairs, 2019, p. 22.

[14] Czech Republic. Statement by Mr. Richard Kadlčák at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of United Nations, 2020, p. 3.

[15] New Zealand. The Application of International Law to State Activity in Cyberspace, 2020, p. 2.

salīdzinājumā ar kritēriju, kas balstīts tikai uz novērojamām materiālām sekām, sniedz nepārprotamas priekšrocības paredzamības ziņā, tādējādi veicinot juridisko noteiktību. Atšķirībā no "uz sekām balstītas" pieejas, kur veiksmīgas uzlaušanas operācijas ietekme var nebūt uzreiz redzama vai var paiet laiks, kamēr tā materializējas, saskaņā ar "uz ielaušanos vērstu" pieeju pats uzbrucēju uzlaušanas akts ir suverenitātes pārkāpums.[16] Līdz ar to cietušajai valstij nav jāgaida, kad parādīsies fiziskas sekas, lai būtu juridiski pamatoti īstenot pretpasākumus. Šāda pieeja uzsver kiberdrošības pārvaldības proaktīvo raksturu, dodot valstīm iespēju ātri un izlēmīgi reaģēt uz uztvertajiem draudiem digitālajā jomā. Šī ierosinātā pieeja ir guvusi atbalstu valstu starpā, Francijas valdībai norādot, ka suverenitātes pārkāpums var pastāvēt pat tad, kad notiek iekļūšana Francijas datorsistēmās. Ņemot vērā, ka iekļūšana notiek tad, ja tiek pārkāpta informācijas drošība, proti, cietušās valsts sistēmas konfidencialitāte, integritāte vai pieejamība, tā ir līdzīga iepriekš norādītajai "uz ielaušanās vērstai" pieejai. Pieņemot šādu pieeju, valsts atzīst, ka pārkāpums ir noticis ikreiz, kad uzbrucējs veic "neatļautu iekļūšanu Francijas sistēmās vai jebkādu seku radīšanu Francijas teritorijā, izmantojot digitālo vektoru"[17].

Redzams, ka starptautisko tiesību interpretācija kibertelpā ir ievērojami attīstījusies, taču vienprātības trūkums starp valstīm par teritoriālās suverenitātes piemērošanu kibertelpā norāda uz piemērotu brīdi jaunu koncepciju izpētei un apspriešanai. Forumi, kā ANO Atvērtās dalības starpvaldību darba grupas vai Valdību ekspertu grupas, ir piemēroti, lai pētītu jaunas idejas un izskatītu atšķirīgus viedokļus. Abos forumos valstīm ir iespējas apspriest normu un principu izstrādi attiecībā uz valstu atbildību kibertelpā, iespējamiem sadarbības pasākumiem un to, kā starptautiskās tiesības piemērojamas kibertelpā. Piemēram, pirmā Atvērtā darba grupa radīja precedentu debatēm par starptautisko kiberdrošību – sesijā piedalījās 193 valstis un vairāk nekā 100 nevalstisko organizāciju pievienojās kā novērotājas.[18] Tāpat Valdību ekspertu grupa ir plaši izmantots mehānisms, lai pētītu jaunus tematus un izstrādātu ieteikumus, kas varētu būt pamatā turpmākām sarunām par starptautisku līgumu vai citu vienošanos. Valdību ekspertu grupa darbojas, pamatojoties uz konsensu,[19] kas varētu apgrūtināt vienota projekta izstrādi, taču vienprātība neapšaubāmi ir svarīga leģitimitātes nodrošināšanai. Ņemot vērā kiberdrošības izaicinājumu dinamisko raksturu un straujo tehnoloģiju attīstības tempu, valstīm ir aktīvi jāiesaistās diskusijās, lai kopīgi izvērtētu un formulētu savu nostāju jautājumos, kas attiecas uz suverenitāti kibertelpā, un veicinātu visaptverošākas sistēmas izstrādi.

---

[16] Roguski P. Violations of Territorial Sovereignty in Cyberspace: an Intrusion-Based Approach. In: Broeders D., Berg B. (eds). Governing Cyberspace: Behavior, Power, and Diplomacy, Rowman & Littlefield, 2020, pp. 79–80.

[17] Lahmann H. On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace. Duke Journal of Comparative & International Law, Vol. 32, 2021, p. 87; Ministère des Armées, 2019, p. 6.

[18] Hurel L. M. The Rocky Road to Cyber Norms at the United Nations. Council on Foreign Relations, 6 September 2022. Pieejams: https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0 [aplūkots 20.03.2025.]

[19] ICT4Peace Foundation. Remarks by Dr. Daniel Stauffacher, Founder and President, ICT4Peace to Jeju Forum, 2019. Pieejams: https://ict4peace.org/wp-content/uploads/2019/11/ICT4Peace-2019-OEWG-UN-GGE-How-to-live-with-two-UN-processes.pdf [aplūkots 20.03.2025.]

2. Starptautiskās atbildības attiecināšanas problemātika

Tradicionālajos militārajos konfliktos ar kinētiskiem uzbrukumiem uzbrucēju identificēt ir salīdzinoši vienkārši. Taču kiberoperāciju gadījumā šāda attiecināšana ir daudz sarežģītāka – lai pierādītu, ka konkrēta valsts ir kiberoperācijas iniciatore, ir nepieciešami pierādījumi, kuru iegūšana bieži vien ir ārkārtīgi sarežģīta vai pat neiespējama.

Tallinas rokasgrāmata 2.0 paredz, ka kiberoperāciju var attiecināt uz valsti, ja tā ir veikta pēc valsts norādījumiem, tās vadībā vai kontrolē vai ja valsts šo operāciju ir atzinusi un pieņēmusi kā savu. Lai konstatētu atbilstību "vadības vai kontroles" nosacījumam, starptautiskā ekspertu grupa par piemērotāko atzina ANO Starptautiskās tiesas efektīvās kontroles testu, kas izmantots Nikaragvas un Bosnijas genocīda lietās.[20] Saskaņā ar efektīvās kontroles testu atbildīgajai valstij ir ne tikai jāsniedz vispārējs atbalsts, bet arī jādod norādījumi attiecībā uz noteiktām operācijām.

Atsevišķi eksperti tomēr uzskata, ka pašreizējie attiecināšanas testi ir jāpārskata, lai starptautiskās tiesības atspoguļotu dinamisko mijiedarbību starp valstīm un nevalstiskajiem dalībniekiem. Attiecībā uz "kontroles" kritēriju eksperti norāda, ka ANO Starptautiskās tiesību komisijas Pantu par valsts atbildību 8. pants precīzi nenosaka tā darbības jomu, un komisija aicina to interpretēt elastīgi. Turklāt tā ir atzinusi nepieciešamību pēc diferencētām attiecināšanas pieejām, norādot, ka katrs gadījums ir jāvērtē individuāli.[21] Tāpat jāņem vērā arī vēsturiskais konteksts – Pantu par valstu atbildību 8. pantā izklāstītie attiecināšanas kritēriji tika formulēti laikā, kad valstis konfliktos izmantoja bruņotas grupas, kur tās paļāvās uz valstu vadību un resursiem,[22] taču šobrīd pastāvošā realitāte, ņemot vērā kibertelpas attīstību, ir citādāka, tāpēc attiecināšanas testus var uzskatīt par novecojušiem.

Daži autori par piemērotu uzskata vispārējās kontroles testu, kas neprasa pierādīt valsts ieguldījumu katrā atsevišķā darbībā atšķirībā no efektīvās kontroles testa.[23] Lai gan vispārējās kontroles tests paplašina gadījumu loku, kad kiberoperāciju var attiecināt uz valsti, tomēr tas pilnībā neatrisina visas ar attiecināšanu saistītās problēmas. Viena no iespējamām pieejām ir atteikšanās ne tikai no efektīvās kontroles testa, bet arī no vispārējās kontroles testa, tādējādi vēl vairāk pazeminot atbildības slieksni kiberoperāciju gadījumos. Ja pašreizējais regulējums nosaka tik augstu pierādīšanas slieksni, ka valstīm kļūst gandrīz neiespējami juridiski pamatot atbildību par kiberuzbrukumiem, pastāv risks, ka tās meklēs alternatīvus, ārpus tiesiskā regulējuma esošus risinājumus. Pārmērīgi augsts attiecināšanas slieksnis ne tikai vājina starptautiskās atbildības mehānismus, bet arī var veicināt slēptas atriebības kiberoperācijas, tādējādi apdraudot uz noteikumiem balstītu starptautisko kārtību.

---

[20] ANO Starptautiskās tiesas 27.06.1986. spriedums lietā "Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)", Merits, ICJ Reports 1984; ANO Starptautiskās tiesas 16.02.2007. spriedums lietā "Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)", ICJ GL No. 91.

[21] ANO Starptautisko tiesību komisijas pantu "Valstu atbildība par starptautiski prettiesisku rīcību" komentāri, p. 48. Pieejams: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [aplūkots 20.03.2025.]

[22] Tsagourias N., Farrell M. Cyber Attribution: Technical and Legal Approaches and Challenges. European Journal of International Law, Vol. 31, Issue 3, 2020, p. 961.

[23] Tsagourias N., Farrell M. 2020, p. 962.

Attiecināšanas sliekšņa pazemināšana gan paplašina iespējas saukt valstis pie atbildības par kiberoperācijām, taču vienlaikus rada būtiskus riskus – īpaši kļūdainas attiecināšanas draudus, kas var novest pie nepamatotiem atbildes triecieniem un eskalācijas. Kibertelpa ir dinamiska un strauji attīstās, tāpēc pārāk konservatīva pieeja attiecināšanai var nesaskanēt ar tehnoloģiskās vides straujo attīstību. Pārāk šaura interpretācija dod priekšrocības uzbrucējiem, jo rada situāciju, kurā tie var rīkoties nesodīti. Tajā pašā laikā nav arī pamatoti attiecināt uz valsti jebkuru kiberoperāciju, kas īstenota no tās teritorijā esošiem tīkliem.[24]

Ūna Hetaveja (*Oona Hathaway*) ir kritizējusi pašreizējo regulējumu par tā nepietiekamo efektivitāti, norādot, ka tas ļauj valstīm izvairīties no atbildības, ja tās deleģē kiberoperācijas nevalstiskiem aktoriem un saglabā tikai minimālu kontroli pār to darbībām.[25] Savukārt Pīters Marguliss (*Peter Margulies*) uzsver, ka esošais regulējums ne tikai neveicina tiesisko noteiktību, bet arī var pamudināt potenciālās upuru valstis pašām īstenot slēptas taktikas, piemēram, nolīgt privātus kiberspeciālistus, tādējādi vēl vairāk saasinot globālo nestabilitāti.[26]

Ņemot vērā šos argumentus, ir būtiski pārskatīt un pilnveidot valstu atbildības doktrīnu, pielāgojot attiecināšanas mehānismus mūsdienu izaicinājumiem kibertelpā. Lai novērstu nesodāmību zema līmeņa (*below-the-threshold*) kiberoperāciju gadījumos, būtu pamatoti atteikties no efektīvās kontroles testa un pazemināt attiecināšanas slieksni, ieviešot pieeju, kas tuvāka vispārējās kontroles modelim. Piemēram, cietušajai valstij vajadzētu pierādīt, ka uzbrucējvalsts sniegusi būtisku atbalstu kiberoperācijas īstenošanai, nodrošinot ļaunprātīgu programmatūru, kas izmantota uzbrukumā, vai aktīvi iesaistoties kiberoperācijas plānošanā un izpildē. Tomēr, lai saglabātu līdzsvaru un novērstu pārmērīgu attiecināšanas kritēriju atvieglošanu, izšķirošais faktors būtu pierādījumi par nozīmīgu valsts iesaisti kiberoperācijas organizēšanā un īstenošanā.

Kopsavilkums

1. Valstis atzīst, ka suverenitātes princips ir piemērojams kibertelpā, tomēr nepastāv vienprātība par to, vai suverenitāte darbojas kā patstāvīga tiesību norma, kuru iespējams pārkāpt. Lai kiberoperāciju varētu uzskatīt par starptautisko tiesību pārkāpumu saskaņā ar suverenitātes kā principa pieeju, tai būtu jāpārkāpj militārā spēka lietošanas aizlieguma vai iejaukšanās aizlieguma princips. Šāda interpretācija paplašina to ļaunprātīgo darbību loku, kas kibertelpā paliek nesodītas. Tādējādi nesankcionēta piekļuve kiberinfrastruktūrai, datu iegūšana no valdības vai privātiem tīkliem netiek automātiski uzskatītas par suverenitātes pārkāpumu.
2. Precīzas teritoriālās integritātes pārkāpuma robežas nav definētas. Tomēr valsts suverenitātes un teritoriālās integritātes aizskārums ir neapstrīdams, ja kiberoperācija ietekmē kritisko infrastruktūru vai kiberinfrastruktūru, izraisot fizisku

[24] Margulies P. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. Melbourne Journal of International Law, Vol. 14, 2013, p. 5.

[25] Hathaway O., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W., Spiegel J. The Law of Cyber-Attack. California Law Review, Vol. 100, No. 4, 2012, pp. 546–547.

[26] Margulies P. 2013, p. 5; Tran D. The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack. The Yale Journal of Law & Technology, Vol. 20, 2018, p. 419.

kaitējumu vai tās funkcionalitātes zudumu. Līdz ar to valstīm ir pamats pieņemt pieeju, koncentrējoties uz jebkādu nesankcionētu ielaušanos savā kiberinfrastruktūrā, nevis tikai uz tās radītajām sekām. Šāda pieeja ļauj valstīm savlaicīgi identificēt un novērst potenciāli kaitīgas darbības, pirms tās materializējas.

3. Valstīm ir jāpieņem nostāja par suverenitātes piemērošanu kibertelpā, publiski darot to zināmu un sniedzot piemērus, kas palīdz noteikt robežas suverenitātes pārkāpumiem. Lai gan ES līmenī dalībvalstis ir vienojušās par starptautisko tiesību piemērošanu kibertelpā, šis jautājums jāattīsta forumos, piemēram, ANO Atvērtās dalības starpvaldību darba grupās vai Valdību ekspertu grupās. Šajos formātos valstis var apspriest tālāku normu, principu un atbildības mehānismu izstrādi, kā arī sadarbības pasākumus kiberdrošības jomā.
4. Lai gan efektīvas kontroles tests joprojām ir dominējošais juridiskais standarts, tiek atzīts, ka šī testa piemērošana kibertelpā var būt pārāk stingra un neveicina efektīvu atbildības piemērošanu. Neskatoties uz priekšlikumiem aizstāt to ar alternatīviem testiem, piemēram, vispārējās kontroles testu vai citiem zemākiem standartiem, tie līdz šim nav guvuši plašu atbalstu starp valstīm. Tomēr atteikšanās no efektīvās kontroles testa var būt pamatota, jo tā stingrās prasības var veicināt nesodāmību zema līmeņa kiberoperāciju gadījumos.