Univerza v Ljubljani
Pravna fakulteta
Katedra za mednarodno pravo

MEDNARODNOPRAVNI VIDIKI EKONOMSKEGA VOHUNJENJA V KIBERNETSKEM PROSTORU

(magistrsko diplomsko delo)

Pika Šarf

Mentorica:
izr. prof. dr. Vasilka Sancin

Ljubljana, november 2016

POVZETEK

Mednarodnopravni vidiki ekonomskega vohunjenja v kibernetskem prostoru

Pika Šarf

Mentorica: izr. prof. Vasilka Sancin

Namen magistrskega diplomskega dela je obravnava mednarodnopravne ureditve ekonomskega kibernetskega vohunstva in predstavitev spremenjenih potreb držav, ki so vodile do razvoja in bliskovitega porasta te vrste vohunstva v zadnjih nekaj letih. Strnjeno je predstavljen spor zaradi obtožb ZDA, da Kitajska izvaja dejavnosti ekonomskega kibernetskega vohunstva. Mednarodnopravna ureditev ekonomskega kibernetskega vohunstva je obravnavana s treh zornih kotov. Prvi del je namenjen obravnavi vprašanja, ali je vohunstvo *per se* v mednarodnem pravu dovoljeno ali prepovedano. V drugem delu je analizirana dopustnost ekonomskega kibernetskega vohunstva z vidika nekaterih splošnih načel mednarodnega prava, še posebej načela ozemeljske suverenosti in načela nevmešavanja. Ob tem je poudarjeno, da mednarodno pravo ureja tudi ravnanje držav v kibernetskem prostoru. Zadnji del diplomske naloge je namenjen obravnavi ekonomskega kibernetskega vohunstva v okviru Svetovne trgovinske organizacije. V tem delu je podrobneje predstavljena organizacijska struktura WTO in postopek za reševanje sporov WTO. Obravnavane so določbe Sporazuma o trgovinskih vidikih pravic intelektualne lastnine, katerih kršitev bi države članice, ki so tarča ekonomskega kibernetskega vohunstva, lahko zatrjevale v postopku za reševanje sporov WTO. Magistrsko diplomsko delo se zaključi z ugotovitvijo, da bi nova pravila mednarodnega prava, ki bi uredila ekonomsko kibernetsko vohunstvo zagotovo prinesla več jasnosti, vendar pa je zelo malo verjetno, da bi države dosegle soglasje glede tega vprašanja.

Ključne besede: ekonomsko kibernetsko vohunjenje, kibernetski prostor, načelo ozemeljske suverenosti, načelo neintervencije, Svetovna trgovinska organizacija.

ABSTRACT

International law perspectives on economic espionage in cyberspace

Pika Šarf

Mentor: Associate Professor Vasilka Sancin PhD

The purpose of this master's thesis is to discuss international law regulation of economic cyber esiponage and to present the changes in the needs of states that led to development and rapid increase of this type of espionage in the recent years. A dispute over allegations of the USA that China is conducting economic cyber espionage is briefly presented. The position of economic cyber espionage in international law is dealt with from three different perspectives. The first part is aimed at addressing the question whether espionage *per se* is permitted or prohibited under international law. The second part analyzes the accordance of economic cyber espionage with the existing norms of international law, in particular with the principle of territorial sovereignty and principle of non-intervention. It has to be emphasized, that international law governs the conduct of states in cyberspace. The last part of the thesis is aimed at discussion of the problem of economic cyber espionage within the World Trade Organisation. The relevant provisions of the Agreement on Trade-Related Aspects of Intellectual Property Rights will be presented, the the violation of which could be claimed in the dispute settlement procedure by the WTO Member states, which are targets of cyber economic espionage. Master's thesis is concluded with a finding that new norms of international law designed specifically to regulate cyber economic espionage would bring more clarity, however, it is very unlikely that the states would reach a consensus on this issue.

Key words: economic cyber espionage, cyberspace, principle of territorial sovereignty, principle of non-intervention, World Trade Organisation.

Zahvala

Družini, za brezpogojno podporo in zaupanje v času študija.

Oskarju, za potrpljenje in oporo v trenutkih, ko se mi je zdelo, da se ne da več naprej.

In mentorici, izr. prof. Vasilki Sancin, za pomoč pri pisanju magistrske naloge, neprecenljivo znanje in veselje do mednarodnega prava.

The spy of the future is less likely to resemble James Bond, whose chief assets were his fists, than the Line X engineer who lives quietly down the street and never does anything more violent than turn a page of a manual or flick on his microcomputer.

Alvin Toffler, Power Shift: Knowledge, Wealth, and Violence at the Edge of The 21st Century

OKRAJŠAVE

DSB	Dispute Settlement Body
DSS	Dispute Settlement System
DSU	Dispute Settlement Understanding
GATT	General Agreement on Tariffs and Trade
ICJ Rep.	International Court of Justice Reports
NATO CCD COE	North Atlantic Treaty Organisation Cooperative Cyber Defence Centre of Excellence
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation
NSA	National Security Agency
OZN	Organizacija združenih narodov
RIAA	Reports of International Arbitral Awards
TRIPS	(The Agreement on) Trade-Related Aspects of Intellectual Property Rights
USA	United States of America
UN Doc.	United Nations Document
WIPO	World Intellectual Property Organisation
WTO	World Trade Organisation
ZDA	Združene države Amerike

ed.	editor
nav. delo	navedeno delo
npr.	na primer
odst.	odstavek
str.	stran
t. i.	tako imenovan
tj.	to je

KAZALO

1. UVOD

Leta 2010 je bil Dongfan Chun, inženir, ki je med drugim sodeloval pri razvoju Boengovih letal in razvoju vesoljskih plovil ameriške vesoljske agencije NASA, v ZDA obsojen na 15 let zaporne kazni zaradi ekonomskega vohunjenja.[1] V njegovi hiši so našli več kot 250.000 zaupnih dokumentov, ki jih je v več kot 30 letih, ki jih je preživel kot vohun, posredoval kitajski letalski industriji. Zaseženi dokumenti so zavzeli prostornino več kot štirih omar.[2] Enako količino dokumentov bi Donfan Chun ob prelomu tisočletja lahko shranil na eno zgoščenko, nekaj let kasneje pa na USB ključ manjši od konice prsta.[3] Danes bi Dongfan Chun do podatkov dostopal anonimno iz varnega zavetja svojega doma na Kitajskem. Izkoristil bi prednosti, ki jih je prinesel razvoj informacijsko-komunikacijske tehnologije in verjetno ga ne bi nikoli odkrili.

Vohunstvo ni nov pojav, prav nasprotno, nekateri mu pripisujejo naravo drugega najstarejšega poklica.[4] V zadnjih letih smo priča silovitemu porastu vohunstva, ki mu je nov zagon omogočil razvoj informacijsko-komunikacijske tehnologije. Vsesplošna selitev dejavnosti iz resničnega, fizičnega sveta v kibernetski prostor je kmalu pokazala svoje prednosti – kraja zaupnih podatkov je v kibernetskem prostoru razmeroma hitra in enostavna, predvsem pa je na tak način mogoče do podatkov

[1] Dongfan Chun je prvi ameriški državljan, ki je bil v ZDA obsojen zaradi ekonomskega vohunjenja. FBI Audio, Donfan "Greg" Chun, dostopno na: https://www.fbi.gov/audio-repository/news-podcasts-gotcha-dongfan-greg-chung.mp3/view (18. 10. 2016).

[2] Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, okrober 2011, dostopno na: https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (18.10.2016); A new Kind of Spy, How China Obtains American Technological Secrets, dostopno na: http://www.newyorker.com/magazine/2014/05/05/a-new-kind-of-spy (18. 10 .2016).

[3] Ob predpostavki, da en znak v enostavnem urejevalniku besedila zavzame približno en bajt, bi za eno stran besedila potrebovali 2 kilobajta, za 250.000 pa 500.000, kar je enako 488 megabajtov. Kapaciteta ene zgoščenke je 700 megabajtov, USB ključi za domačo uporabo pa imajo danes že kapaciteto do 1 terabajta. Če dodamo še podatek, da je cena takega USB ključa v povprečju četrt dolarja na gigabajt, nam postane jasno, da je lahko danes na izredno enostaven in cenovno dostopen način shranimo nepredstavljive količine podatkov. Za več podatkov o t. i. mini USB ključih glej: What are the Best Mini USB 3.0 USB Drives?, dostopno na: http://www.everythingusb.com/mini-drives.html (18.10.2016). Za več o tem, koliko podatkov zavzame določeno delo glej: Bibliotekarska terminologija: Koliko je en kilobajt, megabajt, gigabajt?, dostopno na: http://terminologija.blogspot.si/2010/11/koliko-je-en-kilobajt-megabajt-gigabajt.html (18. 10 .2016).

[4] Chesterman S., The Spy Who Came in from the Cold War: Intelligence and International Law, 27 Michigan Journal of International Law 1071, 2006, str. 1072.

dostopati oddaljeno in skoraj popolnoma anonimno.[5] Zato ne preseneča, da danes dejavnosti kibernetskega vohunstva že močno prevladajo nad tradicionalnimi oblikami.[6] Posebno veliko grožnjo tako podjetjem, kot tudi gospodarstvom držav, predstavlja ekonomsko kibernetsko vohunstvo, tj. pridobivanje zaupnih ekonomskih podatkov s strani držav in posredovanje teh podatkov domačim podjetjem z namenom pridobivanja ekonomske konkurenčne prednosti. Zaradi pomanjkljivih podatkov o tovrstnih napadih je škodo, ki jo povzročajo, izredno težko oceniti, grobe ocene pa variirajo med nekaj 100 milijardami in trilijonom ameriških dolarjev.[7] Kljub ogromni škodi, ki jo ekonomsko kibernetsko vohunstvo povzroča, se tovrstni napadi nadaljujejo, medtem ko mednarodna skupnost precej neuspešno išče učinkovito rešitev.

Cilj magistrskega diplomskega dela bo odgovoriti na vprašanje, ali je z obstoječimi mehanizmi mednarodnega prava mogoče nasloviti vprašanje ekonomskega kibernetskega vohunstva. Obravnavano vprašanje je del širšega problema mednarodne (ne)zakonitosti vohunjenja v času miru, zato v določenih delih obravnavam vprašanje kot celoto, na drugih mestih pa poskušam opozoriti na razliko med ekonomskim in tradicionalnim, tj. političnim in vojaškim vohunstvom, in njene posledice za mednarodnopravno ureditev. Obenem pa se ob upoštevanju narave kibernetskega prostora in pravne regulacije ravnanj v njem postavlja še eno, za to magistrsko diplomsko delo mnogo preobsežno vprašanje: ali je danes pravo, ne le mednarodno, temveč tudi nacionalno, sploh še sposobno slediti tehnološkemu razvoju? In ali ni vsako pravno pravilo zaradi naglega napredka skoraj v trenutku nastanka že zastarelo?

[5] Bernik I., Prislan K., Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem, Fakulteta za varnostne vede, Univerza v Mariboru, Ljubljana, 2012, str. v.

[6] Buchan R., The International Legal Regulation of State-Sponsored Cyber Espionage, v: Osula A., Rõigas H (ed.), International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications, Talin, 2016, str. 66.

[7] Treba je poudariti, da so vsi podatki, ki kažejo na manjši obseg škode, stari nekaj let. Tovrstna dejavnost iz leta v leto skokovito narašča, venar zaradi narave dejavnosti, ki poteka skrivno in jo je izredno težko odkriti, lahko le ugibamo kakšne so dejanske posledice ekonomskega kibernetskega vohunstva za posamične države in svetovno gospodarstvo. Za več podatkov o škodi, ki jo letno povzroči kibernetska kriminaliteta, vključno z ekonomskim vohunjenjem, glej npr.: Net Losses: Estimating the Global Cost of Cybercrime, dostopno na: http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/rp-economic-impact-cybercrime2.pdf (18. 10. 2016).

Prvi del magistrskega diplomskega dela je namenjen splošni razpravi o spremembah, ki jih je doživelo vohunstvo v zadnjih petdesetih letih, v katerih se je iz tradicionalnega, vojaškega in političnega vohunstva preobrazilo v ekonomsko vohunstvo, ki s pridom izkorišča prednosti kibernetskega prostora za oddaljeno pridobivanje zaupnih podatkov.

V drugem delu predstavim tradicionalne poglede avtorjev na zakonitost vohunstva *per se*, ki jih lahko razdelimo v tri skupine: prvi zagovarjajo stališče, da mednarodno pravo vohunstvo prepoveduje, drugi ravno nasprotno, da je vohunstvo dovoljeno zaradi permisivnega pravila mednarodnega običajnega prava in tretji govorijo o posebnem statusu vohunstva v mednarodnem pravu.

V tretjem delu magistrskega diplomskega dela se najprej posvetim vprašanju uporabe pravil mednarodnega prava za ravnanje držav v kibernetskem prostoru in nadaljujem z analizo skladnosti dejanj ekonomskega kibernetskega vohunstva z obstoječimi normami mednarodnega prava, načelom ozemeljske suverenosti in načelom nevmešavanja.

V zadnjem delu preučujem možnost reševanja vprašanja ekonomskega kibernetskega vohunstva v okviru Svetovne trgovinske organizacije (World Trade Organisation, v nadaljevanju WTO). V tem delu so podrobneje predstavljena pravila mednarodnega trgovinskega prava, ki bi bila lahko primerna za urejanje ekonomskega kibernetskega vohunstva in postopek reševanja sporov v WTO, v katerem bi države te kršitve lahko uveljavljale. Magistrsko diplomsko delo zaključim z ugotovitvijo, da je zaradi narave vohunstva zelo malo verjetno, da bi države kdaj na mednarodni ravni s sprejemom multilateralne pogodbe prepovedale vohunstvo. Ker pa gre za vedno bolj pereč problem, lahko pričakujemo, da bodo države tudi v prihodnje lažje urejale to vprašanje bilateralno, bodisi s sklepanjem nezavezujočih prijateljskih dogovorov, bodisi da se bodo odločile za korak naprej in sklenile mednarodno pogodbo.

Zaradi odsotnosti uradne opredelitve kibernetskega vohunjenja bom za potrebe magistrskega diplomskega dela uporabila naslednjo delovno opredelitev: kibernetsko vohunjenje je prikrito pridobivanje javno nedostopnih podatkov, ki so začasno ali trajno shranjeni za računalniški infrastrukturi, ki se nahaja na ozemlju druge suverene

države s strani države oziroma akterjev, katerih dejanja so pripisljiva državi. Definicija izpostavlja dejstvo, da v procesu pridobivanja podatkov slednji niso na nikakršen način spremenjeni in dejanja vohunjenja ne vplivajo na dostopnost informacij.[8]

[8] Zelo podobni delovni opredelitvi uporabljata tudi *Ziolkowski* in *Veber*. Ziolkowski K., Peacetime Cyber Espionage – New Tendencies in Public International Law, v: Ziolkowski K. (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Talin, 2013, str. 429; Veber M., Ali kibernetski prostor spreminja mednarodnopravne vidike ekonomskega vohunstva med državami? Pravna praksa, letnik 2016, številka 10, str. 16.

2. VOHUNJENJE – ORIS PROBLEMA

Države danes delujejo v vedno bolj globaliziranem in konkurenčnem okolju, v katerem je njihova uspešnost med drugim odvisna tudi od dostopa do zanesljivih podatkov, ki razkrivajo prednosti in slabosti njihovih konkurentov. Velik del teh podatkov je javno dostopnih, zato njihovo pridobivanje ni sporno.[9] Države pa pogosto na različne načine pridobivajo tudi tajne in javno nedostopne podatke. Delovanje, ki meri na pridobivanje zaupnih gospodarskih, vojaških in drugih podatkov imenujemo vohunjenje.[10]

2.1 Od tradicionalnega k kibernetskemu vohunstvu

Tradicionalno so države informacije pridobivale s pomočjo človeških virov,[11] tako da so na ozemlje tujih držav pošiljale svoje agente. Tehnološki razvoj v zadnjih desetletjih pa je omogočil uporabo učinkovitejših načinov pridobivanja informacij z izkoriščanjem sodobnih tehničnih sredstev, ki predvsem omogočajo oddaljen dostop do podatkov in ne zahtevajo več fizične prisotnosti agenta na tujem ozemlju, s tem pa očitno zmanjšujejo možnost njihovega odkritja in kasnejšega pregona. Razvoj kibernetskega prostora je državam ponudil novo orodje, ki omogoča enostaven, hiter in anonimen dostop do podatkov, ki so bodisi shranjeni na kibernetski infrastrukturi na tujem teritoriju, bodisi jih država prestreže, ko potujejo prek infrastrukture na njenem ali tujem ozemlju.[12] Zaradi tega nekateri dobo interneta že imenujejo "zlata doba vohunstva".[13]

Kibernetsko vohunstvo je pritegnilo svetovno pozornost leta 2013, potem ko je Edward Snowden, bivši pogodbeni sodelavec Agencije za državno varnost ZDA

[9] Buchan R., 2016, nav. delo str. 65.

[10] Slovar slovenskega knjižnega jezika vohunjenje definira kot: "s prikritim poizvedovanjem, iskanjem prizadevati si priti do zaupnih gospodarskih, vojaških podatkov in jih posredovati tuji osebi, državi". Fran, Slovarji Inštituta za slovenski jezik Frana Ramovša ZRC SAZU, Slovar slovenskega knjižnega jezika, geslo: vohuniti, dostopno na: http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=vohuniti&hs=1 (1. 11.2016).

[11] Zbiranje informacij s človeškimi viri imenujemo HUM-INT (human intelligence). Za več o drugih oblikah obveščevalne dejavnosti glej npr. Forcese C., Spies Without Borders: International Law and Intelligence Collection , 5 Journal of National Security Law & Policy 179, 2011, str. 181–182.

[12] Czosseck C., State Actors and Their Proxies in Cyberspace, v: Ziolkowski K. (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Talin, 2013, str. 14.

[13] Ziolkowski K., nav. delo, str. 425.

(National Scurity Agency; v nadaljevanju: NSA) na spletni strani WikiLeaks razkril tisoče zaupnih dokumentov, ki so dokazovali, da NSA že leta sodeluje v globalnem programu množičnega nadzora. Skupaj z državami povezanimi v skupino "Pet oči" (ang. the Five Eyes), ki je nastala kot posledica sporazuma UKUSA[14] iz leta 1946 med ZDA in Veliko Britanijo in je bil sprva namenjen le sodelovanju pri prestrezanju vojaških in političnih informacij v skladu z doktrino povojnega časa, so ZDA desetletja prestrezale in obdelovale elektronske in telefonske komunikacije več milijonov ljudi po vsem svetu.[15] Tarče teh aktivnosti so bili tudi visoki državni predstavniki, med drugim nemška kanclerka Angela Merkel, verski voditelji, številna podjetja ter nevladne organizacije.[16]

2.2 Od vojaškega in političnega k ekonomskemu vohunjenju

Zavedanje, da je stabilnost držav in premoč na vojaškem in političnem področju odvisna tudi od ekonomske nadvlade, je tesno povezano s koncem hladne vojne. Pred tem so bili mednarodni odnosi utemeljeni na vojaških zavezništvih, konec hladne vojne pa je prinesel ne le otoplitev odnosov med vzhodom in zahodom, temveč tudi s tem povezan vzpon mednarodnega trga. Države zato svojih obveščevalnih dejavnosti niso več osredotočale le na zbiranje vojaških in političnih podatkov, temveč so začele pridobivati tudi podatke, ki so ključni za delovanje in poslovanje njihovih podjetij in lahko prispevajo k ekonomski stabilnosti države.[17] Ekonomsko vohunstvo se je razvilo zaradi potrebe po razvoju in večji konkurenčnosti, ki so jo države želele doseči na čim lažji način, pri tem pa so izkoristile pravno podhranjenost tega področja. Ekonomsko vohunstvo, tj. s strani države podprto zbiranje javno

[14] 5. marca 1946 sta Velika Britanija in ZDA v Londonu sklenili sporazum o sodelovanju na področju obveščevalne dejavnosti, takrat znan kot sporazum BRUSA (British-US Communication Intelligence Agreement), ki ga danes poznamo pod imenom UKUSA. Sporazum je bil sklenjen v popolni tajnosti. Mednarodna skupnost je dolgo ugibala o njegovem obstoju, leta 2010 pa sta NSA in britanska obveščevalna služba presenetili in ne le potrdili, da sporazum obstaja, temveč ga tudi v celoti objavili na spletni strani NSA. Not so Secret: Deal at the Heart of UK-US Intelligence, dostopno na: https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released (30.9.2016). Za besedilo celotnega sporazuma glej: UKUSA Agreement Release 1940–1956, dostopno na: https://www.nsa.gov/news-features/declassified-documents/ukusa/ (30.9.2016).

[15] Bernik I., Prislan K., nav. delo, str. 64.

[16] Buchan R., 2016, nav. delo, str. 66–67.

[17] Lotrionte C., Countering State-Sponsored Cyber Economic Espionage Under International Law, 40 North Carolina Journal of International Law and Commercial Regulation 443, 2015, str. 444-445; Sepura K., Economic Espionage: The Front Line of a New Economic War, 26 Syracuse Journal of International Law and Commerce 127, 1998, str. 127-128; Tucker D., The Federal Government's War on Economic Espionage, 18 Journal of International Law 1109, 2014, str. 1109–1110.

nedostopnih podatkov tujih podjetij, ki jih država da na razpolago svojim podjetjem in jim s tem zagotovi strateško ekonomsko prednost, pa moramo razlikovati od industrijskega vohunstva, o katerem govorimo, kadar gre za krajo poslovnih skrivnosti med dvema subjektoma zasebnega prava.[18]

Ekonomsko vohunjenje se ni pojavilo šele v zadnjih petdesetih letih, ampak je pojav star toliko, kot je staro samo vohunstvo. Znan je primer kitajske princese, ki naj bi pred več kot 1500 leti med potovanjem v Indijo tja v laseh pretihotapila sviloprejke in tako izdala stoletja staro skrivnost izdelovanja svile. Prav tako na Kitajskem se je v 18. stoletju francoski jezuit izučil izdelovati kitajski porcelan, skrivni postopek pa potem v pismih razkril francoskim izdelovalcem.[19] Tudi do enega največjih sporov v zgodovini matematike med angleškim fizikom Isaacom Newtnom in nemškim filozofom in matematikom Gotfriedom Wilhelmom Leibnizem zaradi izuma kalkulusa (t. i. infinitezimalni račun; ang. calculus) je prišlo zaradi Newtonowih obtožb o kraji ideje, ki je bila plod domnevno več let trajajočega vohunskega projekta, katerega cilj je bil prenos tujih idej v Nemčijo, ki bi si za ta odkritja potem lahko lastila zasluge.[20]

Tako kot tradicionalno vohunjenje se tudi ekonomsko vohunjenje v zadnjem desetletju seli v kibernetski prostor. Dostop do informacij je postal sofisticiran in prikrit, zato se včasih poraja občutek, da ga sploh ni, medtem ko je realnost ravno nasprotna, saj smo priča izrazitemu porastu kibernetskega ekonomskega vohunstva.[21] Coca-Cola, Adobe, Google, Yahoo in SolarWorld so le nekatera izmed podjetij, ki so javno priznala, da so bila tarča kibernetskega vohunstva.[22] Za mnoge druge vdore javnost zaradi strahu podjetij pred izgubo zaupanja strank nikoli ne bo izvedela,[23]

[18] Fidler D., Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies, American Society of International Law, Insights 17, 2013, str. 1.

[19] Sepura K., nav. delo, str. 130.

[20] Sastry S. S., The Newton-Leibniz Controversy over the Invention of the Calculus, str. 3, dostopno na: http://pages.cs.wisc.edu/~sastry/hs323/calculus.pdf (30. 9. 2016).

[21] Bernik I., Prislan K., nav. delo, str. 81.

[22] Lotrionte C., nav. delo, str. 454.

[23] Podjetja prijavijo le 5-10 odstotkov vdorov v njihove računalniške sisteme. Večinoma je razlog v tem, da se podjetja bojijo negativnega vpliva na njihov sloves, kar bi lahko vplivalo tako na stranke, ki bi se preusmerile k varnejšim konkurentom, kot tudi pri kotiranju na borzi. Za več glej npr. Bernik I., Prislan K., nav. delo, str. 77.

mnoga podjetja pa zaradi nezadostne zaščite računalniških sistemov takšnih napadov sploh ne zaznajo.[24] Nekateri zato zatrjujejo, da je ekonomsko kibernetsko vohunstvo že povzročilo "največji prenos premoženja v zgodovini"[25].

2.3 Kibernetsko ekonomsko vohunstvo: primer ZDA in Kitajske

ZDA so svetovna politična, vojaška in gospodarska velesila, obenem pa država, ki je izredno odvisna od komunikacijske infrastrukture, zato ne preseneča, da so najpogostejša tarča vdorov v informacijske sisteme. Prav tako so na udaru podjetja v ZDA, ki so v zadnjih letih vedno pogosteje žrtve kraje zaupnih ekonomskih podatkov. Na drugi strani se kot državo izvora takšnih napadov največkrat omenja Kitajska, ki tudi na nedovoljene načine skuša nadoknaditi zaostanek v razvoju in tako doseči ostale svetovne gospodarske velesile. [26] Le nekaj mesecev pred razkritji Edwarda Snowdna je februarja 2013 ameriška družba Mandiant, eno izmed takrat vodilnih podjetij na področju programskih rešitev za zagotavljanje varnosti, izdala poročilo, v katerem je razkrila dokaze, ki so neposredno povezovali kibernetske napade posebne enote kitajske vojske, imenovane Enota 61398, na ameriška podjetja.[27] Ni skrivnost, da Kitajska uri elitno skupino računalničarjev za "bojevanje" v kibernetskem prostoru, vendar je Mandiantovo poročilo prvo potrdilo obstoj posebne enote, ki se ukvarja prav z ekonomskim kibernetskim vohunstvom.

Tudi na podlagi tega razkritja so ZDA leta 2014 obtožile pet pripadnikov kitajske vojske na podlagi Zakona o ekonomskem vohunstvu ZDA[28]. Obtoženi naj bi od leta 2006 vdirali v računalniške sisteme podjetij v ZDA in pridobivali zaupne podatke, ki so predstavljali konkurenčno prednost in jih izročali podjetjem na Kitajskem.[29] Tako so ZDA postale ena prvih držav, ki je javno obtožila akterje, katerih ravnanja so

[24] Bernik I., Prislan K., nav. delo, str. 78.

[25] American Enterprise Institute: Cybersecurity and American Power, Addresing New Threats to America's Economy and Military, Keynote Address, Gen. Keith B. Alexander, dostopno na: https://www.aei.org/events/cybersecurity-and-american-power/ (30. 9. 2016).

[26] Bernik I., Prislan K., nav. delo, str. 87.

[27] Mandiant, APT 1: Exposing One of China's Cyber Espionage Units, dostopno na: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (30. 9. 2016).

[28] Economic Espionage Act, Pub.L. 104-294, 110 Stat. 3488, enacted October 11, 1996, dostopno na: https://www.gpo.gov/fdsys/pkg/PLAW-104publ294/html/PLAW-104publ294.htm (30. 9. 2016).

[29] United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui, Indictment, United States District Court, Western District of Pennsylvania, dostopno na: https://www.justice.gov/iso/opa/resources/512201451913235846194 9.pdf (30. 9. 2016).

pripisljiva državi, zaradi ekonomskega kibernetskega vohunstva, vendar pa je šlo za relativno neuspešen poskus ZDA, da bi opozorile mednarodno skupnost na to problematiko[30].

Korak naprej na področju kraje ekonomskih podatkov je pomenila sklenitev prijateljskega dogovora, ki sta ga sklenila predsednika ZDA in Kitajske Barack Obama in Ši Džinping septembra 2015 v katerem sta se obe strani zavezali, da ne bosta izvajali ali podpirali ekonomskega kibernetskega vohunstva.[31] Klub temu, da gre za prijateljski dogovor, ki ne ustvarja mednarodnopravnih zavez, pomeni pomemben premik naprej, ne le za umiritev mednarodnih odnosov med ZDA in Kitajsko, temveč tudi ker kaže na zavedanje velesil, da je vprašanje ekonomskega vohunstva potrebno urediti na mednarodni ravni.[32] Na žalost so se opozorila mnogih, da dogovor ne bo dosegel želenih rezultatov, izkazala za resnična, potem ko je podjetje CrowdStrike, ki zagotavlja varnost številnih ameriških podjetij, le dan po sklenitvi dogovora sporočilo, da je že zaznalo in uspešno preprečilo kibernetski napad iz sistemov, ki so zagotovo povezani s kitajskimi oblastmi.[33]

Vendar niso vsi izgledi tako črni. V letu od sklenitve dogovora je število napadov z namenom kraje podatkov na podjetja v ZDA vendarle upadlo, so pa napadi vedno bolj izpopolnjeni in posledično težje zaznavni.[34] Poleg tega je Kitajska podoben dogovor sklenila še z Veliko Britanijo[35], pogaja pa se tudi z Nemčijo[36]. Podporo

[30] Fidler D., U.S.-China Cyber Deal Takes Norm Against Economic Espionage Global, dostopno na: http://blogs.cfr.org/cyber/2015/09/28/u-s-china-cyber-deal-takes-norm-against-economic-espionage-global/ (30. 9. 2016).

[31] The White House, Office of the Press Secretary, september 2015: Fact Sheet: President Xi Jinping's State Visit to the United States, dostopno na: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (30. 9. 2016).

[32] Veber M., nav. delo, str. 17.

[33] The Latest on Chinese-Affiliated Intrusions into Commercial Companies, dostopno na: https://www.crowdstrike.com/blog/the-latest-on-chinese-affiliated-intrusions-into-commercial-companies/ (30.9.2016).

[34] FireEye Special Report: Red Line Drawn, China Recalculates its Use of Cyber Espionage, dostopno na: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf (1. 10. 2016).

[35] Xi Jinping State Visit: UK and China Sign Cybersecurity Pact, dostopno na: https://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron (1. 10. 2016).

[36] China Working to Halt Commercial Cyberwar in Deal with Germany, dostopno na: http://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany (1. 10. 2016).

prizadevanjem za prepoved kibernetskega ekonomskega vohunstva so izrazili tudi voditelji držav združenih v skupino G20 v končnem poročilu vrha v Antalyi.[37] Nagla reakcija ostalih držav, ki jo je sprožil prijateljski dogovor med Kitajsko in ZDA tako morda le nakazuje na možnost, da se bodo države v bližnji prihodnosti sporazumele in tudi na mednarodni ravni prepovedale ekonomsko kibernetsko vohunstvo.

[37] G20 Leaders' Communique, Antalya Summit, november 2015, dostopno na: http://www.consilium.europa.eu/en/press/press-releases/2015/11/16-g20-summit-antalya-communique/ (1. 10. 2016).

3. MEDNARODNOPRAVNA UREDITEV VOHUNSTVA

Mednarodno pravo v le v omejenem obsegu ureja vohunstvo v okviru prava oboroženih spopadov,[38] njegov status v času miru pa je na mednarodnopravni ravni nejasen. Falk je opozoril, da

"*mednarodno pravo pozablja na dejavnost vohunstva v času miru, saj številne razprave vohunstvo bodisi v celoti prezrejo ali pa vsebujejo le površen odstavek z definicijo vohuna in opisom njegove nesrečne usode ob prijetju*".[39]

Zaradi odsotnosti dokončnega in enotnega odgovora o zakonitosti vohunstva v mednarodnem pravu, obstaja več različnih in nasprotujočih si stališč glede tega vprašanja. V grobem jih lahko razdelimo v tri skupine: prva zagovarja tezo o prepovedi vohunstva v mednarodnem pravu, druga zagovarja stališče o oblikovanju pravila mednarodnega običajnega prava, ki vohunstvo dovoljuje, tretja trdi, da vohunjenje v mednarodnem pravu uživa poseben status, zato ni mogoče vzpostaviti niti njegove zakonitosti niti nezakonitosti.[40]

Forcese se zavzema za drugačen pristop in popolnoma opusti razpravo o tem, ali je vohunjenje *per se* dovoljeno ali ne in se preusmeri na preučevanje posameznih ravnanj in kako le-ta kršijo pravila mednarodnega prava, na primer načelo ozemeljske suverenosti, načelo nevmešavanja in pravila diplomatskega in konzularnega prava.[41]

V tem delu izhajam iz tradicionalnega pristopa, torej, ali je vohunjenje *per se* zakonito ali ne. V njem obravnavam položaje tradicionalnega, kot tudi kibernetskega in ekonomskega kibernetskega vohunstva v mednarodnem pravu kot enake, saj gre glede ciljev za bistveno podobno dejavnost, kibernetsko vohunstvo pri tem le izrablja

[38] 46. člen Dodatnega protokola I k Ženevskim konvencijam iz leta 1949 o zaščiti žrtev mednarodnih oboroženih spopadov iz leta 1977 ureja status vohunov, ujetih v oboroženih spopadih.

[39] Falk R. A., Foreword to Essays on Espionage and International Law, v: Stanger R.J.(ed.), Essays on Espionage and International Law, Ohio State University Press, 1962, str. v.

[40] Radsan J. A., The Unresolved Equation of Espionage and International Law, 28 Michigan Journal of International Law 595, 2007, str. 601; Ziolkowski K., nav. delo, str. 430–431.

[41] Forcese C., Pragmatism and Principle: Intelligence Agencies and International Law, 102 Virginia Law Review 67, 2016, str. 68.

sodobno informacijsko in komunikacijsko tehnologijo,[42] na koncu poglavja pa se opredelim glede razlike med tradicionalnim in ekonomskim vohunjenjem, ki ga zagovarjajo nekatere države.

3.1 Teoretična izhodišča, ki vohunstvo razglašajo za prepovedano po mednarodnem pravu

Stališče starejše teorije je, da mednarodno pravo vohunstvo prepoveduje.[43] Maloštevilni avtorji, ki zagovarjajo mednarodno prepoved vohunstva priznavajo, da je takšno stališče izredno sporno in da obstajajo številni argumenti, ki dokazujejo nasprotno.[44] To stališče je utemeljeno na premisi, da je vohunstvo kaznivo po nacionalnem pravu večine držav, zato ga prepoveduje tudi mednarodno pravo. Temelji torej na predpostavki, da "*če bi bilo v mednarodnem pravu nekaj resnično zakonito (ali vsaj ne bi bilo nezakonito), ne bi nobena država preganjala tistih, ki so to storili*"[45]. Taka utemeljitev pa temelji na napačnem razumevanju splošnih načel mednarodnega prava kot vira mednarodnega prava.

Splošna pravna načela[46] so načela, ki jih vsebujejo posamezni nacionalni pravni sistemi in so tako pomembna, da je njihova veljavnost pogoj za obstoj sistema, poleg tega pa so skupna vsem pravnim redom. Predvsem so v pomoč drugim pravnim virom pri zapolnjevanju pravnih praznin. Kadar je takšno načelo mogoče uporabiti za odnose med državami, najdejo svoj pozitivnopravni izraz v mednarodnem pravu.[47] Nacionalna kazenska zakonodaja, ki inkriminira vohunstvo ureja individualno kazensko odgovornost posameznikov, zato prepoved na nacionalni ravni ne more voditi v prepoved vohunjenja v mednarodnem pravu, katerega subjekti so države in ne

[42] Lewis J.A., The Cyber War has Not Begun, Center for Strategic and International Studies, 2010, str. 2, dostopno na: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100311_TheCyberWarHasNotBegun.pdf (4. 10. 2016).

[43] Garcia Mora M. R., Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition, 26 University of Pittsburgh Law Review 65, 1964, str. 78; Delupis I., Foreign Warships and Immunity for Espionage, 78 American Journal of International Law 53, 1984, str. 67.

[44] Garcia Mora M. R., nav. delo, str. 79–80.

[45] Radsan J. A., nav. delo , str. 604.

[46] Med splošna pravna načela štejemo načelo *ne bis in idem*, načelo dobre vere (*bona fides*), načelo polne odškodnine, neupravičeno obogatitev in druge.

[47] Brownlie I., Principles of Public International Law, Oxford University Press, New York, 2008, str. 16–17; Türk D., Temelji mednarodnega prava, IUS Software, GV Založba, Ljubljana, 2015, str. 49.

posamezniki. Prav tako ni mogoče trditi, da gre pri prepovedi vohunstva za načelo domačega prava, brez katerega bi bil ogrožen sam obstoj pravnega sistema.[48]

Vprašanja, ali mednarodno pravo vsebuje prepoved vohunstva tudi ne smemo enačiti z vprašanjem o morebitni protipravnosti predhodnih ravnanj[49] in prepovedjo uporabe določenih metod ali sredstev v procesu pridobivanja informacij, kot je na primer prepoved mučenja,[50] saj gre za ločeni vprašanji, ki na prepoved samega vohunstva v mednarodnem pravu ne vplivata.

3.2 Teoretična izhodišča, ki vohunstvo razglašajo za dovoljeno po mednarodnem pravu

Številni avtorji zagovarjajo nasprotno stališče, da države tiho sprejemajo zakonitost vohunstva kot pravilo mednarodnega običajnega prava.[51] Nekateri vohunjenje v času miru celo priznavajo kot legitimno funkcijo države in bistveni del mednarodnih odnosov[52]. Že na začetku 20. stoletja je *Oppenheim* pisal o razširjeni praksi pošiljanja vohunov v tujino v prepričanju, da tovrstno ravnanje "ni niti moralno, niti politično ali pravno sporno".[53] Obseg državnega vohunjenja se je od takrat močno povečal in dosegel svoj vrh v času informacijske in komunikacijske tehnologije,[54] vendar so se države vseskozi na vohunstvo odzivale le tako, da so osebo, ki je vohunsko dejavnost opravljala, razglasile za *persona non grata*[55] ali pa so na svojem teritoriju ujete vohune na skrivaj izmenjale za svoje vohune, ki so bili ujeti v tujini.[56] *Smith* in *Yoo* zato menita, da se je na podlagi dolgotrajne prakse držav, ki so ob tem, ko so postale tarče vohunstva, ostale pasivne in niso zatrjevale njegove mednarodne protipravnosti,

[48] Ziolkowski K., nav. delo, str. 432.

[49] Prav tam, str. 431.

[50] Lotrionte C., nav. delo, str. 481.

[51] Yoo J., Sulmasy G., Counterintuative: Intelligence operations and International Law, 28 Michigan Journal of International Law 625, 2006, str. 628; Smith J.H., Symposium: State Intelligence Gathering and International Law, Keynote Address, 28 Michigan Journal of International Law 543, str. 544; McDougal M. S., Lasswell H. D., Reisman W. M., The Intelligence Function and World Public Order, 46 Faculty Scholarship Series 365, 1973, str. 395.

[52] Smith J. H., nav. delo, str. 544; Baker C. D., Tolerance of International Espionage: A Functional Approach, 19 American University International Law Review 1091, 2003, str. 1092.

[53] Oppenheim L., International Law, A Treatise, Longman, Greens & Co., London 1905, str. 491.

[54] Ziolkowski K., nav. delo, str. 425.

[55] Brown G., Poellet K., The Customary International Law of Cyberspace, 6 Strategic Studies Quarterly 126, 2012, str. 133; Forcese C., 2011, nav. delo., str. 200.

[56] Lotrionte, nav. delo., str. 461.

niti niso sprožile nobenih pravnih postopkov, izoblikovalo pravilo mednarodnega običajnega prava, ki določa dopustnost vohunstva.[57]

Za nastanek pravila mednarodnega običajnega prava morata biti kumulativno izpolnjena dva pogoja, objektivni pogoj razširjene prakse držav in subjektivni, zavest subjektov mednarodnega prava s katero sprejemajo to prakso kot zavezujočo.[58] Danes je razširjenost prakse vohunjenja med državami nesporna, večina avtorjev se pri tem sklicuje na dejstvo, da države podpirajo delovanje svojih obveščevalnih služb kot legitimne funkcije države, njihova naloga pa je tudi pridobivanje zaupnih podatkov iz tujine, s tem pa implicitno priznavajo prakso vohunjenja.[59] Vendar pa lahko le javna praksa držav vpliva na nastanek novega pravila običajnega prava.[60] Ker je vohunjenje po sami definiciji skrivna dejavnost, to prikrito delovanje ne more pripeljati do nastanka novega pravila običajnega prava.

Poleg razširjene prakse držav mora biti za nastanek norme običajnega mednarodnega prava izpolnjen tudi subjektivni pogoj, ki se kaže kot zavest držav (*opinio juris sive necessitatis*), da je norma obvezujoča. Države, ki so tarče vohunstva pogosto javno protestirajo, da vohunjenje mednarodnemu pravu nasprotuje, kar dokazuje, da vohunjenje spremlja zavest o mednarodni protipravnosti in ne obratno. Posebej očitno se je to pokazalo po razkritjih Edwarda Snowdna, ko so mnoge države izrazile nasprotovanje praksi NSA, Brazilija se je pri tem tudi jasno sklicevala na kršitev pravil mednarodnega prava[61]. Enako stališče so leto kasneje zavzele tudi ZDA, ko so se kljub odsotnosti sklicevanja na kršitev pravil mednarodnega prava odzvale na napad na podjetje Sony z uvedbo ekonomskih sankcij proti domnevni napadalki

[57] Yoo J., Sulmasy G., nav. delo, str. 628.

[58] North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands), [1969] I.C.J. Rep.3, §77; Brownlie I., nav. delo, str. 6–9.

[59] Ziolkowski K., nav. delo, str. 438; Smith J.H., nav. delo , str. 544.

[60] Second Report on the Identification of Customary International Law, International Law Commission UN Doc. A/CN.4/672, 22. 5. 2014, odst. 47.

[61] Brazilian President: US Surveillance a »Breach of International Law«, dostopno na: https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance (3. 10. 2016).

Severni Koreji.[62] Ker je takšen protiukrep mednarodnopravno dopusten le kot odgovor na predhodno kršitev pravil mednarodnega prava,[63] je očitno, da tudi ZDA dejanja vohunjenja razumejo kot kršitev mednarodnega prava.[64] Prav tako se države, ki so soočene z obtožbami vohunjenja ne branijo z zatrjevanjem, da mednarodno pravo vohunstvo dovoljuje, pač pa odgovornosti za tako ravnanje nočejo sprejeti ali pa se na take očitke sploh ne odzivajo.[65] Ob odsotnosti zavesti držav, da jim mednarodno pravo vohunjenje dovoljuje, tudi ob izjemno razširjeni in enotni praksi držav ne more nastati novo pravilo mednarodnega običajnega prava, ki bi dovoljevalo vohunstvo.

3.3 Teoretična izhodišča, ki vohunstvu priznavajo poseben mednarodnopravni status

Izhodišče za tretje stališče izhaja iz načela, ki ga je oblikovalo Stalno medddržavno sodišče v primeru *Lotus*, in sicer da je ravnanje, ki ga mednarodno pravo izrecno ne prepoveduje, *a contrario* dovoljeno.[66] Sodišče je v sodbi zaključilo, da država uživa široko polje diskrecije, znotraj katerega lahko svobodno ravna, razen v primeru, ko je določeno ravnanje izrecno prepovedano s pravili mednarodnega prava.[67] Načelo *Lotus* postane relevantno, kadar mednarodno pravo določenega vprašanja ne ureja. Mednarodno pravo ne vsebuje norme, ki izrecno prepoveduje vohunjenje, zato številni avtorji v načelu *Lotus* vidijo vodilo za razrešitev vprašanja zakonitosti oziroma nezakonitosti vohunjenja.[68] Pri presoji tega vprašanja *Scott* ugotavlja, da je

[62] Malawer S., Chinese Economic Cyber Espionage, U.S. Litigation in the WTO and Other Diplomatic Remedies, Georgetown Journal of International Affairs, 2015, str. 7; Cyberwar and Sony, dostopno na: http://blogs.law.unc.edu/ncilj/2015/01/21/cyberwar-and-sony/ (3.10.2016) ; More Sanctions on North Korea after Sony Case, dostopno na: http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html?_r=0 (3. 10. 2016).

[63] Prvi odstavek 49. člena Pravil o odgovornosti držav za mednarodno protipravna dejanja, Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, GA OR, 56th Sess., UN Doc. A/RES/56/83.

[64] Buchan R., 2016, nav. delo, str. 84–85.

[65] Prav tam, str. 83; Ziolkowski K., nav. delo, str. 441.

[66] Zaradi omejenost prostora se ne bom podrobneje ukvarjala s spornostjo tega načela v mednarodnem pravu. Naj omenim le, da je Meddržavno sodišče kasneje večkrat obravnavalo to načelo in tudi izrecno izrazilo nestrinjanje z njim. Glej npr. svetovalno mnenje Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, [1996], I.C.J. Rep.226, §21–22; Case Concerning Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium), [2002] I.C.J. Rep.63, skupno ločeno mnenje sodnikov Higgins, Kooijmans in Buergenthal, §49–51.

[67] Case of the S.S. "Lotus" (France v. Turkey), [1927], P.C.I.J. (Ser.A)No. 10, str. 19.

[68] Deeks A., An International Legal Framework for Surveillance, 55 Virginia Journal of International Law 291, 2014, str. 301; Ziolkowski K., nav. delo, str. 446; Radsan J. A., nav. delo, str. 605.

položaj vohunstva v mednarodnem pravu tako nejasen, da ne moremo zaključiti niti da je dovoljeno, niti da je prepovedano.[69]

Baker dopolni načelo *Lotus* s funkcionalnim pristopom, na podlagi katerega vohunstvo razume kot orodje za spodbujanje mednarodnih odnosov in krepitev zaupanja med državami. Pridobivanje informacij s pomočjo vohunjenja državi omogoči, da lahko vedno preveri resničnost podatkov, ki ji jih države posredujejo, zato so države prej pripravljene stopiti v mednarodne odnose. Poleg tega lahko na ta način vedno preverijo, ali se druge države držijo prevzetih mednarodnih obveznosti.[70] Kljub temu, da *Baker* zagovarja, da mednarodno pravo niti ne dovoljuje, niti ne prepoveduje vohunjenja, je njegov pristop bližje teorijam, ki zagovarjajo zakonitost vohunjenja.

Meddržavno sodišče se nikoli ni opredelilo do morebitne zakonitosti vohunjenja v mednarodnem pravu. Čeprav je vsaj v primeru *Diplomatskega in konzularnega osebja ZDA v* Teheranu imelo to priložnost,[71] se z vprašanjem ni ukvarjalo. O vprašanju zakonitosti vohunjenja bi sodišče ob drugače postavljenem zahtevku Nikaragve lahko odločalo tudi v primeru *Vojaških in paravojaških aktivnosti v Nikaragvi,* saj se je Nikaragva pritožila tudi zaradi preletov ameriških letal z namenom zbiranja podatkov, [72] vendar pa je Nikaragva zatrjevala le kršitev načela ozemeljske suverenosti. [73] Ker Meddržavno sodišče lahko odloča le v okviru postavljenih zahtevkov,[74] se o zakonitosti vohunstva v tem primeru ni moglo izreči.

---

[69] Scott R. D., Territorially Intrusive Intelligence Collection and International Law, 46 Air Force Law Review 217, 1999, str. 223.

[70] Baker C. D., nav. delo, str. 1104–1105.

[71] Sodišče je odločilo, da zaradi pomanjkanja dokazov nima nikakršne podlage za odločanje o navedbah iranskega zunanjega ministra Ayatollaha Khomeinija, ki je v več javnih izjavah vztrajal, da je diplomatsko in konzularno predstavništvo ZDA v Teheranu središče vohunske dejavnosti ZDA v Iranu, in s tem upravičeval zasedbo predstavništva in zadrževanje talcev. United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), [1980], I.C.J.Rep.3, §82.

[72] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA), Merits, [1986] I.C.J. Rep.14, §22.

[73] Prav tam, §87, 250.

[74] Gre za t. i. pravilo *non ultra petitia*, o katrem je sodnik *Buergenthal* zapisal: "... a cardinal rule which does not allow the Court to deal with a subject in the *dispositif* of its judgment that the parties to the case have not, in their final submissions, asked it to adjudicate." Oil Platforms (Islamic Republic of Iran v. United States of America), Separate Opinion of Judge Buergenthal, [2003] I.C.J.Rep.270, §3.

Vendar pa odsotnosti pravil, ki izrecno prepovedujejo vohunjenje ne moremo enačiti s skladnostjo vohunskih dejavnosti z mednarodnim pravom. Kot bo prikazano v nadaljevanju, vohunstvo vsaj po mnenju nekaterih avtorjev, lahko krši nekatera pravila mednarodnega prava, predvsem načelo ozemeljske suverenosti držav in načelo nevmešavanja, posebej v povezavi z ekonomskim kibernetskim vohunstvom pa tudi pogodbene določbe s področja mednarodnega trgovinskega prava.

3.4 Razlikovanje med pravno ureditvijo tradicionalnega in ekonomskega vohunstva

ZDA vztrajajo, da mednarodno pravo ekonomsko vohunstvo prepoveduje, tradicionalnega pa ne. Tradicionalno vohunstvo, torej pridobivanje vojaških ali političnih podatkov, prispeva k ohranjanju svetovanje varnosti in je utemeljeno na reciprociteti, [75] zato ni mednarodno sporno. Enake koristi pa ne izhajajo iz ekonomskega kibernetskega vohunstva, saj slednje vedno povzroči korist ene države na škodo druge. Država, ki izvaja dejavnost ekonomskega vohunstva pridobi znanje ali informacije, s katerimi lahko izniči konkurenčno prednost države tarče.[76] Postavlja se vprašanje, ali je na podlagi praktičnih razlik med tradicionalnim in ekonomskim vohunstvom dejansko prišlo do različne mednarodnopravne ureditve.

Kot dokaz razlikovanja med tradicionalnim in ekonomskim vohunjenjem *Lotrionte* navaja različen odziv držav na ti dve obliki vohunjenja. Države so običajno vohune bodisi razglasile za *persone non grate*, bodisi so sklenile skriven dogovor o izmenjavi agentov. Obtožba petih pripadnikov kitajske vojske zaradi ekonomskega vohunjenja v kibernetskem prostoru je prekinila to prakso. ZDA, ki so se odločile za obtožbo, kljub temu, da je zelo malo verjetno, da bo Kitajska pripravljena sodelovati z ZDA in izročiti svoje državljane, so poslale jasen signal, da ekonomskega vohunjenja ne bodo

[75] Mednarodno pravo temelji na načelu reciprocitete. Države vstopajo v mednarodne dogovore na podlagi prepričanja, da se bodo vse strani držale svojih mednarodnih obveznosti in tako bo tak dogovor vsem vpletem državam v korist. Tudi vohunjenje ponuja obema vpletenima državama koristi, ker državam omogoča, da preverijo namere druge države in s tem krepijo zaupanje in spodbujajo mednarodno sodelovanje, obenem pa državnim organom zagotavljajo potrebne informacije za optimalne odločitve. Lotrionte C., nav. delo, 2015, str. 482–483; Chesterman S., nav. delo, str. 1090.

[76] Lotrionte C., nav. delo, str. 488; Parajon Skinner C, An International Law Response to Economic Cyber Espionage, 46 Connecticut Law Rewiew 1165, 2014, str. 1184.

tolerirale. Potrebno pa je poudariti, da se ZDA nikoli niso sklicevale na kršitev mednarodnega prava, temveč samo na kršitev notranjega prava.[77]

Vendar pa, nasprotno z ZDA, prevladujoči del teorije in večina v mednarodni skupnosti ekonomsko in tradicionalno vohunjenje obravnava enako,[78] zato v magistrskem diplomskem delu ne bom razlikovala med obema oblikama, razen če bo to posebej navedeno in pa v poglavju o kršitvi pravil WTO, ki velja posebej samo za ekonomsko kibernetsko vohunstvo.

[77] Pirker B., Territorial Sovereignty and Integrity and the Challenges of Cyberspace, v: Ziolkowski K. (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Talin, 2013, str. 202.

[78] Fidler D., 2013, nav. delo, str. 3; Danielson M.E.A., Economic Espionage: A Framework for a Workable Solution, 10 Minnesota Journal of Law, Science & Technology 503, 2009, str. 514; Merkin K., Critical Analysis: Economic Espionage and International Law, dostopno na: http://djilp.org/4721/critical-analysis-economic-espionage-and-international-law/ (4. 10. 2016).

4. EKONOMSKO KIBERNETSKO VOHUNSTVO KOT KRŠITEV OBSTOJEČIH PRAVIL MEDNARODNEGA PRAVA

Niti mednarodna skupnost, niti mednarodni pravniki ne soglašajo povsem, katera ravnanja v kibernetskem prostoru kršijo pravila mednarodnega prava in eno izmed odprtih in izredno spornih vprašanj ostaja kibernetsko vohunstvo. Zagotovo bi sprejem mednarodnopravnih pravil, ki bi posebej uredila pravice in dolžnosti držav v kibernetskem prostoru prinesel več normativne jasnosti. V trenutni situaciji, ko se soočamo z odsotnostjo specialnih pravil pa je za razjasnitev vprašanja, kako se obstoječa pravila mednarodnega prava uporabijo za ravnanje držav v kibernetskem prostoru je izrednega pomena mnenje priznanih mednarodnih pravnikov. Med sicer razpršenimi razpravami, ki so se v zadnjih letih močno razbohotile, naj izpostavim Talinski priročnik uporabljivega prava za področje kibernetskega vojskovanja (Tallinn Manual on the International Law Applicable to Cyber Warfare, v nadaljevanju: Talinski priročnik), ki je nastal na pobudo zveze NATO in je rezultat več let trajajoče študije mednarodnega prava oboroženih spopadov in uporabe sile, kot se uporabljajo za ravnanje držav v kibernetskem prostoru. Talinski priročnik odgovarja na ključna vprašanja *jus ad bellum* in *jus in bello*, drugih področij mednarodnega prava pa se dotika le toliko, kolikor so relevantna v kontekstu kibernetskega vojskovanja. Priročnik, ki sicer ni pravno zavezujoč dokument, vsebuje 95 pravil s komentarjem, ki postavljajo institute mednarodnega prava kot so prepoved uporabe sile, pravica do samoobrambe in mednarodna odgovornost držav za protipravna dejanja v kontekst kibernetskega prostora.[79]

Pravni strokovnjaki, ki so pripravili Talinski priročnik priznavajo, da predstavljata kibernetsko vohunstvo in kraja intelektualne lastnine z izkoriščanjem kibernetskega prostora resnično in resno grožnjo vsem državam in zato zahtevata ustrezen odziv tako na državni, kot tudi mednarodni ravni. Vendar ti dve področji igrata izredno majhno ali sploh nobene vloge v mednarodnem pravu oboroženih spopadov in uporabe sile, zato ju priročnik izrecno ne obravnava. Poudarili pa so, da kibernetski napad, ki ne pomeni uporabe sile, lahko vendarle krši mednarodno pravo, predvsem

[79] Smith M. (ed.), Tallin Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, New York 2013, str. 1–6.

načelo nevmešavanja.[80] Reševanju prav teh vprašanj je namenjen nadaljevalni projekt zveze NATO, Talinski priročnik 2.0, ki naj bi izšel do konca leta 2016, in se bo posvetil aktivnostim države v kibernetskem prostoru v času miru in s tem skladnosti tega ravnanja z načelom ozemeljske suverenosti, načelom nevmešavanja in načelom skrbnega ravnanja držav.[81]

4.1 Kibernetski prostor – pravna praznina ali pravno regulirano območje?

Preden si podrobneje ogledamo, kdaj ravnanje države ali akterjev, katerih dejanja so pripisljiva državi, krši načela ozemeljske suverenosti in načela nevmešavanja v kibernetskem prostoru, moramo razumeti, da mednarodna skupnost in pravna stroka niso od nekdaj soglašali glede tega, ali je kibernetski prostor mogoče pravno regulirati. Vprašanje, ali se tradicionalna pravila in načela mednarodnega javnega prava uporabljajo za ravnanje držav v kibernetskem prostoru, se v ZDA pojavljajo že od konca 20. stoletja, v Evropi pa sta več zanimanja za to vprašanje pritegnila šele kibernetska napada na Estonijo in Gruzijo v letih 2007 in 2008.[82]

Kibernetski prostor je obstajal že preden so države razmišljale o njegovi normativni ureditvi. Izraz kibernetski prostor je prvi uporabil pisec znanstveno fantastične proze William Gibson v svojem romanu Nevromant v začetku osemdesetih let prejšnjega stoletja.[83] V zgodnji dobi njegovega razvoja so si ga predvsem njegovi takratni uporabniki predstavljali kot brezzakonsko področje. *Barlow* je v Deklaracijo neodvisnosti kibernetskega prostora zapisal, da v kibernetskem prostoru ni prostora za pravne koncepte.[84] Za razumevanje tega pogleda na svobodo kibernetskega prostora in interneta kot njegove pomembne komponente je izrednega pomena, da razumemo osnove njegovega razvoja. Ta je bil sprva močno povezan z akademskim okoljem, ki

[80] Prav tam.

[81] NATO Cooperative Cyber Defence Centre of Excellence, Tallin Manual, dostopno na: https://ccdcoe.org/research.html (14. 10. 2016).

[82] Heintschel von Heineg W., Legal Implications of Territorial Sovereignty in Cyberspace, v: Czosseck C., Ottis R., Ziolkowski K. (ed.), 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Talin, 2012, str. 7.

[83] Predpona kiber- je danes vsespošno uporabljena za opis stvari in dejanj, ki so povezani z informacijsko tehnologijo, čeprav se nekateri z njegovo uporabo ne strinjajo. Shackelford S. J., Managing Cyber Attacks in International Law, Business, and Relations: in Search of Cyber Peace, Cambridge University Press, New York 2014, str. xxxi.

[84] Barlow J., A Declaration of Independence for Cyberspace, dostopno na: https://www.eff.org/cyberspace-independence (3. 10. 2016).

mu je preko interneta omogočal izmenjavo znanja in idej. Tudi ko je postal dostopen širšim množicam, je ena njegovih najpomembnejših odlik ostala dosegljivost informacij vsem, ki so bili z računalnikom povezani z omrežjem.[85] Odprtost in dostopnost sta botrovali nastanku izredno liberalnih idej o kibernetskem prostoru in številni pravni strokovnjaki so podpirali idejo, da kibernetski prostor bodisi sploh ne potrebuje regulacije, bodisi da je za njegovo urejanje namesto državne regulative, primernejša zasebna.[86] Idejo je podprl celo takratni predsednik ZDA Bill Clinton, ki je izjavil, da se "*resnični potencial interneta lahko uresniči le z neregulativnim, tržno usmerjenim pristopom*".[87]

Kasneje se je izoblikovalo stališče, da je kibernetski prostor tako kot vesolje in odprto morje skupno dobro oziroma *res communis omnium* [88], območje zunaj suverenosti držav, za katerega velja posebna ureditev izkoriščanja in upravljanja. V rimskem zasebnem pravu so bile to stvari, ki so bile last vseh in niso mogle biti predmet zasebne lastnine, ker je tak način izkoriščanja najbolj koristil skupnosti kot celoti.[89] V tem je tudi smisel mednarodne ureditve skupnega dobra, ki omogoča izkoriščanje v dobro človeštva kot celote, zato je ta koncept predstavljal ustrezno teoretično izhodišče za razumevanje kibernetskega prostora tistim, ki so že sprejemli sodobnejši pristop in priznavali, da kibernetski prostor ni popolnoma brezpravno območje, niso pa še bili pripravljeni priznati, da je ravnanje v kibernetskem prostoru lahko podvrženo enakim pravilom kot ravnanje v fizičnem svetu.[90]

Danes mednarodna skupnost soglaša, da se mednarodno pravo uporablja tudi za aktivnosti v kibernetskem prostoru in s tem zavrača vse starejše teorije o

[85] Bomse A. L., The Dependence of Cyberspace, 50 Duke Law Review 1717, 2001, str. 1722; Brief History of Internet, dostopno na: http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf (3. 10. 2016).

[86] Post D., What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace, 52 Stanford Law Reiew 1439, 2000, str. 1439; Johnson D., Post D., Law and Borders: The Rise of Law in Cyberspace, 48 Stanford Law Review 1367, 1996, str. 48; Segura Serano A., Internet Regulation and International Law, v: Bogdandy A., Rüdinger W. (ed.), Max Planck Yearbook of United Nations Law, Volume 10, Brill Nijhoff, The Hague, 2006, str. 194–195.

[87] Bomse A. L., nav. delo, str. 1718.

[88] U.S. Department of Defense, The Strategy for Homeland Defense and Civil Support, 2005, str.12, dostopno na: http://www.wslfweb.org/docs/usg/homeland.pdf (3. 10 .2016).

[89] Baslar K., The Concept of the Common Heritage of Mankind in International Law, Kluwer Law International, The Hague, 1998, str. 40–41.

[90] Za več o konceptu skupnega dobra, njegovi zgodovini in ideji o uvrstitvi interneta vanjo glej npr.: Segura Serano A., nav. delo, str. 231–260.

brezpravnosti kibernetskega prostora.[91] Kibernetski prostor kot tak res nima fizične pojavnosti in obstaja samo kot virtualni svet, je pa to vseeno okolje, ki ga je ustvaril človek in je kot tak lahko podvržen pravni regulaciji.[92] Ministrstvo za obrambo ZDA je kibernetski prostor opredelilo kot "globalno domeno v informacijskem okolju, sestavljeno iz medsebojno povezanih in soodvisnih omrežij informacijske tehnologije, ki vključujejo internet, telekomunikacijska omrežja in računalniške sisteme".[93] Iz te definicije lahko izluščimo, da je kibernetski prostor sestavljen iz treh nivojev, izmed katerih vsaj enega sestavljajo fizične komponente, kot so računalniki, optični kabli in žice, strežniki, usmerjevalniki, stikala in mnoge druge, katerih glavna naloga je prenos podatkov. Fizična komponenta, brez katere kibernetski prostor ne more delovati ima geografsko dimenzijo in je zato izhodišče za razpravo o pravnih razmerjih, jurisdikciji in odgovornosti v kibernetskem prostoru. [94]

Čeprav si nobena država ne more prilastiti in razširiti izvrševanja svoje suverenosti nad samim kibernetskim prostorom, [95] pa vsaka suverena država kot posledica načela ozemeljske suverenosti na svojem ozemlju uživa pravico do nadzora nad vso kibernetsko infrastrukturo in vsemi aktivnostmi, ki izhajajo iz te infrastrukture, ne glede na to, ali je le-ta v zasebni ali javni lasti.[96]

4.2 Ali ekonomsko kibernetsko vohunstvo krši načelo ozemeljske suverenosti in načelo neintervencije?

Načelo ozemeljske suverenosti držav in njegov korelat, načelo neintervencije (nevmešavanja) sta temeljni načeli mednarodnega prava. Meddržavno sodišče je že v svoji prvi sodbi ob obravnavanju primera *Dogodkov v Krfski ožini* zapisalo, da je med

[91] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24. junij 2013; Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22. julij 2015; Smith M. (ed.), nav. delo, Part A.

[92] Buchan R., 2016, nav. delo, str. 71.

[93] Department of Defense, Dictionary of Military Terms, »Cyberspace«, dostopno na: http://www.dtic.mil/doctrine/dod_dictionary/ (3. 10. 2016).

[94] Tsagourias N., Buchan R., Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, Cheltenham, 2015, str. 15; Joint Publication 3-12(R), Cyber Operations, str. 3, dostopno na: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

[95] Heintschel von Heineg W., nav. delo, str. 9.

[96] Prav tam; Smith M. (ed.), nav. delo, str. 16.

neodvisnimi državami spoštovanje ozemeljske suverenosti osnovni temelj mednarodnih odnosov.[97] Suverenost države ima pozitivni in negativni vidik, pozitivni izraža pravico suverene države do svobodnega ravnanja na svojem ozemlju, na katerem tudi izvršuje vrhovno oblast, negativni vidik pa zahteva spoštovanje enake pravice drugih suverenih držav. Povedano drugače, negativni vidik načela suverenosti se kaže kot prepoved vmešavanja v zadeve, ki so v izključni notranji pristojnosti druge države.[98]

4.2.1 Ali ekonomsko kibernetsko vohunstvo krši načelo ozemeljske suverenosti?

Država uživa suverenost na svojem ozemlju, ki vključuje kopno ozemlje znotraj državnih meja, notranje morske vode, teritorialno morje, zračni prostor nad njimi ter podzemlje pod njimi.[99] Max Huber je pojasnil, da je "suverenost v razmerju do nekega dela zemeljske oble pravica opravljati funkcije države na tem območju ob izključitvi sleherne druge države".[100] Tradicionalno vohunjenje poteka na ozemlju druge suverene države in zahteva prikrit vstop agenta ali naprave, ki omogoča zbiranje podatkov, na tuje državno ozemlje. Nekateri avtorji se zavzemajo za razlago, da že sama prisotnost tujega agenta na ozemlju države, ki na vstop agenta v državo in njegovo delovanje na njenem ozemlju ni privolila, krši ozemeljsko suverenost te države.[101] Tako na primer *Wright* v okviru razprave o tradicionalnem vohunstvu navaja, da

"*v času miru...vohunstvo in v resnici vsaka penetracija tujega agenta na ozemlje države v nasprotju z nacionalnim pravom pomeni tudi kršitev pravil mednarodnega prava, ki od države zahteva spoštovanje ozemeljske celovitosti in politične neodvisnosti druge države*".[102]

Tako široko razlago kršitve načela ozemeljske suverenosti podpira tudi sodna praksa Meddržavnega sodišča in njegovega predhodnika, Stalnega meddržavnega sodišča. V

[97] Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), Merits, [1949] I.C.J. Rep.4, str. 35.

[98] Türk D., 2015, nav. delo, str. 82; Shaw M., International Law, Cambridge University Press, Cambridge, 2008, str. 490.

[99] Military and Paramilitary Activities in and against Nicaragua, §212.

[100] Island of Palmas Case (Netherlands v. United States of America), RIAA, Vol. II, str. 838.

[101] Chesterman S., nav. delo, str. 1082; Heintschel von Heineg W., nav. delo, str. 14.

[102] Wright Q., Espionage and the Doctrine of Non-Intervention in Internal Affairs, v: Stanger R. J.(ed.), Essays on Espionage and International Law, Ohio State University Press, 1962, str. 13.

vseh spodaj navedenih primerih je sodišče ugotovilo kršitev ozemeljske suverenosti samo zaradi vstopa ali prisotnosti tujega agenta ali naprave, na primer ladje ali letala, na ozemlju tuje suverene države, v katerega ta država ni privolila. Iz tega sledi, da sodišče meni, da za nastanek kršitve ozemeljske suverenosti ni nujno, da nastane materialna škoda. V zadevi *Lotus* je Stalno meddržavno sodišče izreklo, da "ob odsotnosti pravila, ki to izrecno dovoljuje, država ne sme izvrševati svojih funkcij v kakršnikoli obliki na ozemlju druge države".[103] Meddržavno sodišče je v primeru *Dogodkov v Krfski ožini* ugotovilo kršitev ozemeljske suverenosti Albanije zaradi nedovoljenega vstopa vojaških ladij Velike Britanije v albansko teritorialno morje.[104] Prav tako je ugotovilo kršitev načela ozemeljske suverenosti v primeru *Vojaških in paravojaških aktivnosti v Nikaragvi* zaradi preletov izvidniških letal ZDA v zračnem prostoru Nikaragve.[105]

Kot posledica suverenosti nad vsemi fizičnimi komponentami kibernetskega prostora na ozemlju države nekateri avtorji štejejo vsak kibernetski napad na infrastrukturo na ozemlju tuje države za kršitev ozemeljske suverenosti slednje,[106] zagotovo pa je kršitev podana v primeru, če napad povzroči veliko materialno škodo ali žrtve. Ni pa jasno, ali tudi napad manjše intenzitete, ki škode ne povzroči, ali pa je le-ta neznatna krši načelo ozemeljske suverenosti.[107] Lahko bi argumentirali, da je nastanek materialne škode v kontekstu kibernetskih napadov irelevanten, saj lahko tak napad kljub temu da res ne povzroči neposrednega nastanka škode, vseeno povzroči posledice, si so zaznavne – vzemimo kot primer napad na borzo, ki lahko močno prizadene gospodarsko stabilnost države.[108] Med take manj invazivne kibernetske aktivnosti spada tudi ekonomsko kibernetsko vohunjenje, zato lahko zaključimo, da v mednarodni skupnosti ne obstaja soglasje o tem, ali vohunjenje, ki ne vključuje

[103] Case of the S.S. "Lotus" (France v. Turkey), [1927], P.C.I.J. (Ser.A) No.10, str. 18.

[104] Corfu Channel, str. 35.

[105] Military and Paramilitary Activities in and against Nicaragua, §251.

[106] Buchan R., 2016, nav. delo, str. 73; Watts S., Low-Intensity Cyber Operations and the Principle of Non-Intervention, v: Ohlin J. D., Govern K., Finkelstein C. (ed)., Cyber War, Law and Ethic for Virtual Conflicts, Oxford University Press, Oxford, 2015, str. 256.

[107] Smith M. (ed.), nav. delo, str. 16; Heintschel von Heineg W., nav. delo, str. 11.

[108] Ziolkowski K., General Principles of International Law as applicable in Cyberspace, v: Ziolkowski K. (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Talin, 2013, str. 163.

prisotnosti agenta na tujem ozemlju, ampak izkorišča kibernetski prostor za pridobivanje zaupnih ekonomskih podatkov, krši ozemeljsko suverenost.

4.2.2 Ali ekonomsko kibernetsko vohunstvo krši načelo nevmešavanja?

Načelo nevmešavanja ali neintervencije prepoveduje državam samovoljno vmešavanje v zadeve, ki so v pristojnosti druge suverene države. Gre za eno izmed temeljnih načel mednarodnega prava, ki je utemeljeno na suvereni enakosti držav.[109] Njegov status pravila mednarodnega običajnega prava je bil potrjen v več dokumentih OZN,[110] med njimi je najpomembnejša Deklaracija načel mednarodnega prava o prijateljskih odnosih in sodelovanju med državami, v skladu z ustanovno listino OZN,[111] in v več sodbah Meddržavnega sodišča.[112]

Kot pravi *Oppenheim*, je "načelo nevmešavanja posledica pravice vsake države do suverenosti, ozemeljske celovitosti in politične neodvisnosti." [113] Prepoveduje vmešavanje drugih držav v vse "zadeve, za katere je državi zaradi načela suverenosti dovoljeno, da o njih odloča svobodno. Ena izmed njih je izbira političnega, gospodarskega, socialnega in kulturnega sistema in oblikovanje zunanje politike".[114] Kaj natančno sodi v notranje zadeve države, je izredno težko določiti, na splošno pa

[109] Prvi odstavek 2. člena Ustanovne listine OZN (Charter of the United Nations), Uradni list RS –MP, št.1/14.

[110] Generalna skupščina OZN je od leta 1957 sprejela več kot 30 resolucij, ki so naslavljale vprašanje prepovedi intervencije v notranje zadeve držav. Glej npr. Deklaracija o nedopustnosti intervencije v notranje zadeve držav in o zaščiti njihove neodvisnosti in suverenosti (Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, Resolucija Generalne Skupščine OZN, 2131(XX), UN Doc. A/RES/20/2131, 1965; Deklaracija o nedopustnosti intervencije in vmešavanja v notranje zadeve držav (Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of the States), Resolucija Generalne Skupščine OZN, UN Doc. A/RES/36/103, 1981.

[111] Deklaracija načel mednarodnega prava o prijateljskih odnosih in sodelovanju med državami v skladu z ustanovno listino OZN (Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations), Resolucija Generalne Skupščine OZN, 2625(XXV), UN Doc. A/RES/25/2625, 1970.

[112] Military and Paramilitary Activities in and against Nicaragua, §202; Corfu Channel, str. 35; Armed Activities on the Territory of Congo (Democratic Republic of Congo v. Uganda), Judgment, [2005] I.C.J.Rep.168, §161-163.

[113] Jennings R., Watts A. (ed.), Oppenheim's International Law, Volume 1 - Peace, Longman, Harlow, 1992, str. 428.

[114] Military and Paramilitary Activities in and against Nicaragua, §205. Podobno tudi v Deklaraciji načel mednarodnega prava o prijateljskih odnosih in sodelovanju med državami, v skladu z ustanovno listino OZN.: "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law."

velja, da gre za zadeve, ki jih ne ureja niti mednarodno pogodbeno niti običajno pravo.[115] V globaliziranem svetu, v katerem je sodelovanje med državami ključnega pomena, je vedno več področij urejenih z mednarodnim pravom, zato se število zadev, ki so v izključni pristojnosti držav, manjša.[116]

Mejo med bolj ali manj prijateljskim prepričevanjem, ki ga štejemo za normalno sestavino mednarodnih odnosov in samovoljnim, političnim vmešavanjem, ki ga mednarodno pravo prepoveduje, je marsikdaj težko potegniti. V primerih, ko gre za prikrito diplomatsko vmešavanje v zadeve, ki so v pristojnosti druge države, je težko ugotoviti sam dejanski položaj in še težje dokazati, da gre zares za prepovedano intervencijo.[117] V skupnosti, kjer je vsakodnevna komunikacija in stik z drugimi državami bistvenega pomena, se postavlja vprašanje, ki si ga je zastavil že *Wright*:

"Na interese držav vplivajo dejanja drugih držav in slednje skušajo vplivati na ta dejanja. To storijo z razvojem kulture, gospodarstva in moči; z dosežki v tehnologiji, znanosti, literaturi in umetnosti; z mednarodno komunikacijo z uporabo radija, tiska, popularnih in tehničnih revij, s potovanji in trgovanjem svojih državljanov; z uradnimi izjavami, zakonodajno aktivnostjo in diplomatsko korespondenco. Mednarodno pravo se sooča z vprašanjem: kdaj dovoljen vpliv postane prepovedano vmešavanje?"[118]

Razlikovalni element, ki dovoljeni vpliv spremeni v prepovedano vmešavanje, je prisila.[119] Element prisile je po mnenju *Jamnejada* in *Wooda* podan takrat, kadar je

[115] Notranje zadeve države nekateri avtorji enačijo z *domain réservé*, za katero je Stalno meddržavno sodišče v svetovalnem mnenju glede *Dekretov o državljanstvu izdanih v Tuniziji in* Maroku zapisalo:"The words 'solely within the domestic jurisdiction' seem rather to contemplate certain matters which, though they may very closely concern the interest of more than one State, are not, in principle, regulated by international law. (...) The question whether a certain matter is or is not solely within the jurisdiction of a State is an essentially relative question; it depends on the development of international relations." Nationality Decrees Issued in Tunis and Morocco, Advisory Opinion, [1923], P.C.I.J. (Ser.B)No.4, str. 24. Za več o *domain réservé* glej npr. Ziegler K. S., Max Planck Encyclopedia of Public International Law, *Domain Réservé.*

[116] Simma B., Khan D. E., Nolte G., Paulus A. (ed.), The Charter of the United Nations: A Commentary, Volume I, Oxford University Press, Oxford, 2012, str. 291; Kunig P., Max Planck Encyclopedia of Public International Law, Prohibition of Intervention, odst. 3; Watts S., nav. delo, str. 264.

[117] Türk D., Načelo neintervencije v mednarodnih odnosih in v mednarodnem pravu, Mladinska knjiga, Ljubljana, 1984, str. 14.

[118] Wright Q., nav. delo, str. 4–5.

[119] Military and Paramilitary Activities in and against Nicaragua, §205.

"ravnanje ene države usmerjeno v spremembo politike v drugi"[120]. Če država sprejme odločitev za določeno ravnanje, ki ni posledica njene svobodne volje, temveč vpliva druge države, je kršeno načelo nevmešavanja.[121]

Najbolj očiten primer prisile, ki zagotovo povzroči kršitev načela nevmešavanja je prepovedana uporaba sile, vendar pa tudi ravnanja, ki ne vsebujejo direktne fizične prisile lahko kršijo prepoved vmešavanja, kar je potrdilo tudi Meddržavno sodišče v primeru *Vojaških in paravojaških aktivnosti v Nikaragvi*. Načelo nevmešavanja in prepoved uporabe sile sta dve sicer povezani, vendar samostojni načeli mednarodnega prava, ki sta lahko kršeni z enim samim ravnanjem države.[122] Medtem ko uporaba sile vedno pomeni tudi kršitev prepovedi vmešavanja v notranje zadeve države, pa ni tudi vsaka prepovedana intervencija kršitev prepovedi uporabe sile.[123]

Načelo nevmešavanja je lahko kršeno tudi z uporabo političnih, ekonomskih ali diplomatskih sredstev.[124] Obseg ravnanj, ki predstavljajo tovrstno obliko prisile, v mednarodnem pravu ni povsem jasen. Predvsem ravnanja, ki predstavljajo ekonomsko prisilo je izredno težko ločiti od tistih, ki pomenijo le uveljavitev legitimnih gospodarskih interesov države. Med takšna prepovedana ravnanja avtorji prištevajo uvedbo enostranskih ekonomskih sankcij, celovit trgovinski embargo in bojkot.[125]

Prav tako komentar Talinskega priročnika pojasnjuje, da ni vsako kibernetsko vmešavanje že prepovedana intervencija. Kibernetski napad, ki ga izvrši država ali

---

[120] Jamnejad M., Wood M., The Principle of Non-Intervention, 22 Leiden Journal of International Law 345, 2009, str. 347–348.

[121] Ziolkowski K., nav. delo, str. 433.

[122] "acts which breach the principle of non-intervention will also, if they directly or indirectly involve the use of force, constitute a breach of the principle of non-use of force in international relations" Military and Paramilitary Activities in and against Nicaragua, §205, 209; Armed Activities on the Territory of Congo, §164. Zaradi prostorske omejenosti in nerelevantnosti instituta za prepoved ekonomskega kibernetskega vohunstva se v magistrskem diplomskem delu ne bom podrobneje ukvarjala s prepovedjo uporabe sile, ki je sicer eno izmed najpomembnejših načel mednarodnega prava.

[123] Benatar M., The Use of Cyber Force: Need for Legal Justification?, 1 Goettingen Journal of International Law 375, 2009, str.386.

[124] Kunig, nav. delo., odst. 22.

[125] Prav tam, odst. 25, 26; Mattessich W., Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage, 54 Columbia Journal of Transnational Law 873, 2016, str. 880; Benatar M., nav. delo, str. 382.

akterji, katerih ravnanja so pripisljiva državi in je usmerjen proti kibernetski infrastrukturi na teritoriju druge države ter vsebuje element prisile, zagotovo krši mednarodno prepoved nevmešavanja.[126] Kot primer kibernetkega napada, ki krši prepoved nevmešavanja avtorji navajajo DDoS napad (ang. distributed denial of service attack)[127] na Estonijo leta 2007 kot odziv na umik spomenika posvečenega sovjetskemu vojaku v Talinu, ki mu je močno nasprotovala ruska manjšina,[128] in manj znan kibernetski napad na Azerbajdžan leta 2012[129]. Oba kibernetska napada sta bila politično motivirana in usmerjena v spremembo politike v napadeni državi, to pa jasno kaže na prisotnost elementa prisile. Kibernetsko vohunjenje po drugi strani ne krši prepovedi intervencije, ker takšnega elementa prisile ne vsebuje.[130] Sam vdor v računalniški sistem druge države po mnenju strokovnjakov, ki so pripravili priročnik, ne more predstavljati prepovedanega vmešavanja tudi v primeru, če tak vdor zahteva premagovanje zaščitnih ukrepov, na primer prebitje požarnih zidov in krekanje gesel (ang. cracking of passwords).[131]

Nasprotno stališče zagovarja *Buchan,* ki se zavzema za širšo razlago načela neintervencije pri obravnavanju kibernetskega vohunstva. Meni, da načelo nevmešavanja pride v poštev predvsem v tistih primerih, ko so informacije oziroma podatki prestreženi, medtem ko se nahajajo na teritoriju tuje države, bodisi da so

[126] Smith M. (ed.), nav. delo, str. 17.

[127] DDoS napad je oblika kibernetskega napada, pri katerem strežnik, ki gosti določeno spletno stran (ali več spletnih strani), prejme tako veliko zahtev po dostopu v zelo kratkem časovnem obdobju, da to bistveno upočasni njegovo delovanje ali pa delovanje strežnika v celoti onemogoči. Bernik I., Prislan K., nav. delo., str. 168.

[128] 27. aprila 2007 so estonske oblasti prestavile spomenik sovjetskemu vojaku, ki je do tedaj stal v središču estonske prestolnice Talin. Številčna ruska manjšina, ki živi v Estoniji se je odzvala z nasilnimi protesti, ki so jim sledili kibernetski napadi, ki so bili usmerjeni tako zoper vladne spletne strani, kot tudi zoper spletne strani številnih bank in medijev. Ob tem je treba poudariti, da je Estonija tehnološko izredno razvita država, ki je vsaj med evropskimi državami najbolj odvisna od informacijske tehnologije in vpliv kibernetskih napadov, ki so za več kot tri tedne onemogočili dostop do številnih spletnih strani, je imel veliko večji vpliv, kot bi ga imel na delovanje katerekoli druge, manj informacijsko razvite države. Buchan R., Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?, 17 Journal of Conflict & Security Law 211, 2012, str. 218, 225.

[129] Septembra 2012 so bile spletne strani nekaterih vladnih institucij in medijev v Azerbajdžanu tarča kibernetskih napadov, za katere je odgovornost prevzela skupina hekerjev z imenom »Armenska kibernetska vojska«, ki je delovala v skladu z navodili Armenije. Azerbajdžan je ostro obsodil napad in zatrdil, da gre za nadaljevanje konflikta med državama zaradi statusa regije Gorski Karabah. Letter dated 6 September 2012 from the Chargé d'affaires a.i. of the Permanent Mission of Azerbaijan to the United Nations addressed to the Secretary-General, UN Doc. A/66/897-S/2012/687.

[130] Roscini M., Cyber Operations and the Use of Force in International Law, Oxford University Press, New York, 2014, str. 66; Prav tam, str. 44–45.

[131] Prav tam.

shranjeni na kibernetski infrastrukturi na tujem ozemlju ali pa tuj teritorij prečkajo v tranzitu do svoje končne lokacije. Zlahka si predstavljamo, da neka država preko spleta pošlje podatke, ki jih v tranzitu preko infrastrukture na tujem ozemlju zaradi slabe zaščite uspe ukrasti neki tretji državi. Načelo ozemeljske suverenosti v tem primeru državi, ki je lastnica teh podatkov, ne nudi nikakršne zaščite.[132] Kršitev prepovedi nevmešavanja *Buchan* utemelji na ideji o državni suverenosti podatkov[133] in izredno širokemu razumevanju pojma prisile, ki naj bi bil podan v vsakem primeru kraje tujih podatkov, ne glede na to ali tako ravnanje državo sili v delovanje, ki ga ni sama izbrala.[134] Že sam pregled sodne prakse mednarodnih sodišč in tribunalov, kot tudi stališče večinskega dela teorije, ki je predstavljen zgoraj, nam razkrije, da se s takim razumevanjem pojma prisile ni mogoče strinjati, saj je bistveno preširok.

Postavlja se vprašanje, ali je kljub temu, da po večinskem stališču teorije vohunstvo v kibernetskem prostoru ne krši prepovedi vmešavanja zaradi odsotnosti elementa prisile, položaj ekonomskega kibernetskega vohunstva drugačen.

Ekonomsko kibernetsko vohunstvo vključuje krajo zaupnih podatkov, ki pripadajo zasebnim subjektom, vendar pa škoda povzročena tem subjektom negativno vpliva na gospodarstvo države kot celote in s tem na njen položaj na svetovnem trgu. Država, ki je tarča ekonomskega kibernetskega vohunstva, bo zaradi odpravljanja posledic tega škodljivega ravnanja velikokrat prisiljena v spremembo svoje notranje ali zunanje politike, kar po mnenju *Lotrionte* in *Parajon Skinner* posledice te vrste vohunjenja bistveno približa pojmu prisile, kot ga je izoblikovalo Meddržavno sodišče v primeru *Vojaških in paravojaških aktivnosti v Nikaragvi.*[135] Ne glede na to, ali država izkoristi vojaško, diplomatsko ali ekonomsko dimenzijo svoje moči in neodvisno od tega, ali ravna v fizičnem svetu ali kibernetskem prostoru, vmešavanje v notranje ali zunanje

[132] Buchan R., 2016, nav. delo, str. 73

[133] V sporu med Vzhodnim Timorjem in Avstralijo je Vzhodni Timor zatrjeval kršitev suverenosti, ker je Avstralija vdrla v pisarno njihovega agenta in zasegla dokumentacijo, ki se je nanašala na arbitražo med tema dvema državama, ne glede na to, da so bili dokumenti na ozemlju Avstralije. Meddržavno sodišče sicer v sporu ni odločalo, je pa odločilo o začasnih ukrepih, kjer država dokazuje le, ali je zahtevek verjeten. Sodišče je Avstraliji prepovedalo nadaljnje vmešavanje v komunikacijo med Vzhodnim Timorjem in njihovimi odvetniki, kar nekateri avtorji razumejo kot potrditev sodišča, da država uživa suverenost tudi nad podatki, ne glede na to, kje se le-ti nahajajo. Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Provisional Measures, [2014] I.C.J. Rep.147.

[134] Buchan R., 2016, nav. delo, str. 75-81; Tsagourias N., Buchan R., 2016, nav. delo, str. 183–186.

[135] Lotrionte C., nav. delo, str. 503; Parajon Skinner C, nav. delo, str. 1190.

zadeve države, ki vsebuje element prisile, vedno predstavlja prepovedano intervencijo. Tudi nekateri starejši avtorji se strinjajo, da mednarodno pravo prepoveduje ekonomsko prisilo, zlasti kadar jo države izkoriščajo za doseganje politično motiviranih ciljev.[136]

Meddržavno sodišče je v primeru *Vojaških in paravojaških aktivnosti v Nikaragvi* obravnavalo tudi navedbe Nikaragve, da so ZDA prenehale z gospodarsko pomočjo Nikaragvi s tem, da so zmanjšale kvote za uvoz sladkorja za devetdeset odstotkov in uvedle trgovski embargo z namenom oslabitve njenega političnega sistema, s čimer pa so prekršile načelo neintervencije.[137] Sodišče je odločilo, da noben izmed ukrepov tega načela ni kršil.[138] Svoje odločitve sodišče sicer ni podrobneje obrazložilo, vendar lahko razberemo, da so z zmanjšanjem kvot za uvoz sladkorja ZDA zgolj ukinile preferenčno obravnavo Nikaragve in zato niso izvrševale prisile. Prav tako si vsaka država lahko sama izbira svoje trgovinske partnerje, zato tudi trgovinski embargo ne zadosti kriterijem prepovedane intervencije.[139]

Za razliko od situacije v primeru *Vojaških in paravojaških aktivnosti v Nikaragvi* pa dejavnosti ekonomskega kibernetskega vohunstva ne pomenijo zgolj svobodne izbire trgovinskih partnerjev, temveč ciljno in sistematično krajo intelektualne lastnine in drugih zaupnih podatkov, ki gospodarstvu države, ki je tarča takšne aktivnosti, povzroči ogromno škodo, ki bo dolgoročno zagotovo povzročila spremembe v izbiri njene gospodarske politike. Nihče ne oporeka pravici države, da sama izbira ukrepe in metode za vodenje svoje ekonomske politike, dokler se le-te gibljejo v mejah, ki so mednarodnopravno dopustne. Vendar pa določena ravnanja, ki ogrožajo položaj države v svetovni trgovini in lahko vplivajo na njeno ekonomsko neodvisnost in finančno stabilnost, ter v ekstremnih primerih lahko povzročijo grožnjo svetovnemu miru, kršijo načelo neintervencije.[140]

---

[136] Tako stališče zagovarjata na primer *Lillich* in *Bowett*. Za več o tem glej: Lillich R. B., The Status of Economic Coercion Under International Law: United Nations Norms, 12 Texas International Law Journal 17, 1977; Bowett D.W., Economic Coercion and Reprisals by States, 13 Virginia Journal of International Law 1, 1972.

[137] Military and Paramilitary Activities in and against Nicaragua, §22.

[138] Prav tam, §244–245.

[139] Lotrionte C., nav. delo, str. 510-511; Watts S., nav. delo, str. 260-261.

[140] Prav tam.

4.3 Uveljavljanje mednarodne odgovornosti držav za kibernetsko ekonomsko vohunjenje – problem pripisljivosti

Država je odgovorna za mednarodne delikte, ki so v Pravilih o odgovornosti držav za mednarodno protipravna dejanja opredeljeni kot vsako dejanje ali opustitev, ki je pripisljiva državi in pomeni kršitev mednarodne obveznosti države.[141] Ker je država abstrakten pojem in kot taka sama ne more delovati, jo zastopajo njeni organi in ostali, ki delujejo po njenem pooblastilu in za njihovo delovanje je država odgovorna. Država odgovarja za ravnanja vseh svojih organov, ki imajo tak status po notranjem pravu države, ne glede na to, ali organ deluje znotraj svojih pooblastil ali v nasprotju z njimi.[142] Ker država za vedno večje število nalog pooblašča zasebna podjetja in druge entitete, odgovarja tudi za dejanja le-teh, ki sicer niso organi države, vendar delujejo na podlagi pooblastila za opravljanje elementov javne oblasti. Odgovornost države nastane tudi, kadar neka oseba ali skupina dejansko deluje na podlagi navodil ali usmeritev države.[143] Država pa odgovarja tudi, kadar omogoči drugi državi uporabo svojih organov, kadar zaradi opustitve dejavnosti državnih organov državne naloge prevzamejo druge entitete ali kadar je država protipravna dejanja sprejela za svoja, pod določenimi pogoji pa se državi lahko pripišejo tudi odgovornost za ravnanje vstajnikov in drugih gibanj.[144] Posledica mednarodne odgovornosti države je dolžnost države kršiteljice, da s kršitvijo preneha, da zagotovi, da kršitve ne bo ponovila ter ponudi polno reparacijo za materialno in nematerialno škodo.[145]

Danes je nesporno, da se odgovornost držav za mednarodno pravne delikte razteza tudi na njihovo ravnanje v kibernetskem prostoru [146] Države so odgovorne za kibernetske napade, ki jih izvršijo njihovi organi ali drugi akterji, katerih ravnanje je pripisljivo državi.[147] Pri razpravljanju o pravnih vidikih pripisljivosti v kibernetskem prostoru se ne moremo izogniti predhodnim tehničnim vidikom pripisovanja

[141] 1. in 2. člen Pravil o odgovornosti držav za mednarodno protipravna dejanja.

[142] Sancin V., Odgovornost državnih organov za kršitve mednarodnega prava, Javna uprava, 2007, letnik 43, številka 2, str. 510–511.

[143] Kranjc M., Pripisljivost ravnanj izvršenih na podlagi navodil ali usmeritev in nadzora države, diplomsko delo, Ljubljana 2014, str. 11–12.

[144] 4.-11. člen Pravil o odgovornosti držav za mednarodno protipravna dejanja.

[145] 30. in 31. člen Pravil o odgovornosti držav za mednarodno protipravna dejanja.

[146] Smith M. (ed.), nav. delo, str. 29.

[147] Schmitt M. N., Vihul L., Proxy Wars in Cyber Space: The Evolving International Law of Attribution, 1 Fletcher Security Review 55, 2014, str. 58.

določenega ravnanja državi.[148] Brez odgovora na vprašanje, iz katere naprave izvira nedovoljen napad na računalniški sistem ne moremo odkriti storilca mednarodnega delikta in s tem je izključena mednarodna odgovornost države.

Prvič se je vprašanje pripisljivosti za ravnanje v kibernetskem prostoru zastavilo po kibernetskih napadih na Estonijo in Gruzijo, ki so povzročili večdnevno nedostopnost vseh spletnih strani državne uprave in številnih drugih, predvsem bančnih spletnih strani. Čeprav noben izmed napadov ni dobil sodnega epiloga, pa sta obe državi napad pripisovali Rusiji, kar ni presenetljivo, saj sta kibernetska napada časovno sovpadala s sporoma med Rusijo in omenjenima državama.[149] Precej bolj zanimiv z vidika pripisljivosti je virus Stuxnet, najzmogljivejši računalniški virus v zgodovini in prvo kibernetsko orožje, ki mu je (domnevno) uspelo povzročiti škodo v fizičnem svetu. Virus Stuxnet so odkrili leta 2010, potem ko mu je uspelo prodreti v iranski sistem za bogatenje urana Natanz in povečati frekvenco vrtenja jedrskih centrifug do te mere, da so prenehale delovati.[150] Stuxnet naj bi bil le majhen del veliko obsežnejše tajne operacije Nitro Zeus, ki bi stekla v primeru neuspešnih pogajanj o ustavitvi iranskega jedrskega programa.[151] Računalniški analitiki, ki so skušali ugotoviti izvor Stuxneta, so imeli na voljo le kodo, ki ga je sestavljala, ker pa je ta tako sofisticirana,[152] so krog možnih napadalcev lahko zožili na državne akterje v nekaj najrazvitejših državah sveta, ki imajo sredstva za razvoj in testiranje tovrstnih orožij.[153] Na podlagi večletnega preučevanja Stuxneta in pričevanj tako izraelskih kot ameriških visokih

[148] Shamsi J. A., Zeadally S., Sheikh F., Flowers A., Attribution in Cyberspace: Techniques and Legal Implications, 9 Security and Communications Network 2886, 2016, str. 2889.

[149] Allan C. S., Attribution Issues in Cyberspace, 13 Chicago-Kent Journal of International and Comparative Law 55, 2013, str. 58–59

[150] Buchan, 2012, nav. delo, str. 219–220.

[151] Stockburger P. Z., Known Unknowns: State Cyber Operations, Cyber Warfare, and the *Jus Ad Bellum*, 31 American University International Law Review 545, 2016, str. 559; U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict, dostopno na: http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html (3. 11. 2016).

[152] Na izredno dodelanost Stuxneta kaže predvsem izkoriščanje t. i. zero-days ranljivosti, ki se je proizvajelec programske opreme ne zaveda in je zato ne more preprečiti. Gre za izredno redkost v svetu računalniških virusov in le malo je oseb, ki so sposobne ustvariti tako kodo. Kot primer lahko navedem, da so v celem letu 2010 med več milijoni odkritih virusov in črvov odkrili le 12 zero-days ranljivosti, od tega so bile kar štiri v kodi Stuxneta.

[153] Rid T., Buchanan B., Attributing Cyber Attacks, 38 Journal of Strategic Studies 4, 2014, str. 21.

predstavnikov, ki so sodelovali pri razvoju in uporabi Stuxneta,[154] danes lahko z veliko gotovostjo trdimo, da je nastal kot plod sodelovanja med obveščevalnimi službami ZDA in Izraela in je zato pripisljiv tema državama.[155]

Talinski priročnik posveča pravu mednarodne odgovornosti celotno drugo poglavje in podrobneje razlaga, kako se pravila o mednarodni odgovornosti držav uporabijo za njihovo ravnanje v kibernetskem prostoru. Ureja pripisljivost ravnanja državi v dveh situacijah in sicer v primeru kibernetskega napada, ki je bil sprožen s kibernetske infrastrukture v lasti države in kibernetskega napada, ki je preusmerjen preko infrastrukture v lasti države. Kibernetskega napada ni mogoče pripisati državi le na podlagi dejstva, da je napad izviral iz kibernetske infrastrukture v lasti te države, je pa to lahko znak njene vpletenosti. Ravnanja izven kibernetskega prostora lahko pripišemo državi, kadar vpletene osebe uporabljajo državna sredstva, zlasti kadar gre za vojaško opremo, ker je v teh primerih zelo malo verjetno, da bi bila njihova uporaba omogočena komu, za katerega ravnanja ni odgovorna država. Tega klasičnega pristopa v kibernetskem prostoru ni mogoče uporabiti, ker je možnost poneverbe identitete prevelika.[156] Drugačna je situacija, ko kibernetski napad izvira iz računalniškega sistema v eni državi, na poti do svoje tarče pa se prenaša tudi po računalniški infrastrukturi v lasti druge države. Samo dejstvo, da je bila infrastruktura te druge države uporabljena kot sredstvo prenosa, ne more kazati na vpletenost te države v kibernetski napad.[157]

Temeljna značilnost kibernetskega prostora je njegova odprtost, ki je na eni strani omogočila bliskovit razvoj tehnoloških inovacij, po drugi strani pa je botrovala ranljivosti njegovih uporabnikov.[158] Napadalci, ki kibernetski prostor izrabljajo za nezakonite aktivnosti zlahka ostanejo anonimni z uporabo lažne ali ukradene

---

[154] Obama Order Sped Up Wave of Cyberattacks Against Iranhttp://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=3&pagewanted=1&pagewanted=all (9. 11. 2016).

[155] Virus Stuxnet je zaradi svoje skrivnostne in kompleksne narave predmet preučevanja podjetij, ki se ukvarjajo z računalniško varnostjo in številnih raziskovalnih novinarjev. Leta 2016 je izšel dokumentarni film Zero-days, ki podrobno razišče vse okoliščine, ki so spremljele nastanek in pot tega uničevalnega računalniškega virusa.

[156] Smith M. (ed.), nav. delo, str. 34.

[157] Prav tam, str. 36.

[158] Završnik A., Kibernetska kriminaliteta, IUS SOFTWARE, GV Založba, Inštitut za kriminologijo pri Pravni fakulteti, Ljubljana, 2015, str. 21.

identitete, večinoma pa kombinirajo več metod za zagotavljanje anonimnosti.[159] Zaradi posebnosti kibernetskega prostora nekateri avtorji predlagajo tristopenjski postopek ugotavljanja, ali je ravnanje v kibernetskem prostoru mogoče pripisati določeni državi. V prvem koraku se z metodami digitalne forenzike poišče računalnik ali druga elektronska naprava, iz katere napad izvira, v drugem koraku ugotavljamo identiteto uporabnika naprave v trenutku napada in šele v tretjem koraku lahko presojamo, ali je za ravnanje te osebe na podlagi pravil mednarodnega prava odgovorna država.[160]

Na tak način je podjetju CrowdStrike, ki se ukvarja z računalniško varnostjo, uspelo povezati napade na številna podjetja v ZDA s Kitajsko. V prvem koraku so identificirali zlonamernega akterja, ki je pri vseh vdorih v sistem uporabljal vzdevek cpyy. Z analizo podatkov o registraciji so odkrili, da ga uporablja Chen Ping. Preko različnih virov je potem analitikom uspelo pridobiti več slik in drugih podatkov, iz katerih so uspeli izluščiti GPS koordinate računalnika, ki ga je Chen uporabljal. Koordinate so kazale na naslov v Šanghaju, kjer ima svoj sedež Enota 61486, del kitajske vojske, ki je usposobljen posebej za dejavnosti ekonomskega kibernetskega vohunstva.[161] Vsaka aktivnost v kibernetskem prostoru za seboj pušča sledi in tudi najbolje izurjeni uporabniki ne morejo ostati popolnoma anonimni, zato lahko zaključimo, da je postopek ugotavljanja, ali je določeno ravnanje v kibernetskem prostoru pripisljivo državi sicer izredno zahtevno in dolgotrajno, zagotovo pa ne nemogoče.

[159] Shamsi J. A., nav. delo, str. 2888.

[160] Pirker B., nav. delo, str. 212; Roscini M., Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, v: Ohlin J.D., Govern K., Finkelstein C. (ed)., Cyber War, Law and Ethic for Virtual Conflicts, Oxford University Press, Oxford, 2015, str. 220.

[161] Rid T., Buchanan B., nav. delo, str. 13; CrowdStrike Intelligence Report, Putter Panda, dostopno na: https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf (1. 11. 2016).

5. REŠEVANJE SPOROV ZARADI EKONOMSKEGA KIBERNETSKEGA VOHUNSTVO V OKVIRU SVETOVNE TRGOVINSKE ORGANIZACIJE

ZDA kot ena glavnih tarč ekonomskega kibernetskega vohunstva že nekaj časa preučujejo možnost, na katero je leta 2014 opozoril veleposlanik ZDA na Kitajskem Max Bachus,[162] da bi vprašanje kraje zaupnih podatkov reševali v okviru WTO, ker naj bi tako ravnanje pomenilo kršitev nekaterih določb Sporazuma o trgovinskih vidikih pravic intelektualne lastnine (Agreement on Trade - Related Aspects of Intelectual Property Rights, v nadaljevanju sporazum TRIPS) [163] , ki vsebujejo mednarodna pravila o zaščiti intelektualne lastnine.[164] Tudi vedno več mednarodnih pravnikov se zavzema, da bi se spori med državami zaradi ekonomskega kibernetskega vohunstva reševali v okviru postopka za reševanje sporov WTO, katerega glavni prednosti sta širok krog članstva[165] in postopek, ki se po številnih značilnosti približuje sodnemu odločanju in strankama v sporu zagotavlja zavezujočo odločitev.[166]

5.1 Svetovna trgovinska organizacija

WTO je mednarodna organizacija, ki danes igra izjemno pomembno vlogo pri urejanju odnosov v svetovnem gospodarstvu. Čeprav ni vključena v sistem Združenih narodov, jo odlikujeta širok krog članstva in izjemno dovršen sistem kompleksnih in tehnično dovršenih pravil, ki že od začetka njenega delovanja učinkovito urejajo mednarodne trgovinske odnose in naraščajoče konflikte med svetovnimi gospodarskimi velesilami.[167]

---

[162] U.S. Ambassador Baucus says China hacking threatens national security, dostopno na: http://www.reuters.com/article/us-china-usa-baucus-idUSKBN0F00S320140625 (7. 10. 2016).

[163] Sporazum o trgovinskih vidikih pravic intelektualne lastnine (Agreement on Trade – Related Intelectual Property Rights), Uradni list RS – MP, št.10/95.

[164] Strawbridge J., The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation, 47 Georgetown Journal of International Law 833, 2016, str. 836–837.

[165] V WTO je trenutno vključenih 164 držav, med njimi tudi Slovenija. Understanding the WTO, Who we are?, dostopno na: https://www.wto.org/english/thewto_e/whatis_e/who_we_are_e.htm (7. 10. 2016).

[166] Malawer S., nav. delo, str. 2; Lotrionte C., nav. delo, str. 525; Parajon Skinner C, nav. delo, str. 1193-1194.

[167] Peterlin I., Svetovna trgovinska organizacija in državna suverenost, GV Založba, Ljubljana, 2013, str. 110; Understanding the WTO: What is the World Trade Organization?, dostopno na: https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact1_e.htm (7. 10. 2016).

WTO je bila ustanovljena leta 1994 s podpisom Marakeškega sporazuma[168] o ustanovitvi Svetovne trgovinske organizacije (Agreement establishing the WTO, v nadaljevanju: Sporazum o ustanovitvi WTO) kot naslednica Splošnega sporazuma o carinah in trgovini (General Agreement on Tariffs and Trade, v nadaljevanju: GATT)[169]. Tako GATT, ki je osrednji sporazum WTO, kot tudi drugi sporazumi, sprejeti v okviru mehanizma GATT so s tem postali del normativnega reda WTO.

Institucionalno strukturo WTO sestavljajo številni organi, med katerimi sta najpomembnejša ministrska konferenca in generalni svet. Ministrska konferenca (Ministerial Conference) je najvišji organ WTO, ki se sestaja vsaki dve leti. V obdobjih med ministrskimi konferencami WTO dejansko vodi generalni svet (General Council), čeprav deluje pod vodstvom ministrske konference. Generalni svet se sestaja redno, sestavljajo pa ga veleposlaniki, akreditirani pri WTO v Ženevi. Deluje še v dveh drugih vlogah, in sicer kot organ za spremljanje oziroma nadzor trgovinske politike (Trade Policy Review Body) in kot organ za reševanje sporov (Dispute Settlement Body, v nadaljevanju DSB).[170]

Značilnost sprejemanja odločitev v WTO je odločanje s konsenzom, ki je dosežen, če nobena izmed prisotnih držav članic odločitvi ne nasprotuje. Le kadar odločitve ni mogoče sprejeti s konsenzom, pride do glasovanja, v katerem ima vsaka država en glas in se odločitve največkrat sprejmejo z običajno večino. [171]

5.2 Reševanje sporov v okviru Svetovne trgovinske organizacije

Skupaj s preoblikovanjem GATT v WTO leta 1994 so države članice sprejele tudi prilogo k sporazumu WTO, ki je vsebovala Sporazum o pravilih in postopkih za reševanje sporov (Dispute Settlement Understanding, v nadaljevanju: DSU)[172].

[168] Marakeški sporazum o ustanovitvi Svetovne trgovinske organizacije (Marakesh Agreement – Agreement Establishing the World Trade Organisation), Uradni list RS – MP, št.10/95.

[169] Splošni sporazum o carinah in trgovini (General Agreement on Tariffs and Trade 1947), Uradni list RS – MP, št. 4/94.

[170] Türk D., 2015, nav. delo, str. 298; Shaw M., nav. delo, str. 1287.

[171] Prvi odstavek 9. člena Sporazuma o ustanovitvi WTO.

[172] Sporazum o pravilih in postopkih za reševanje sporov (The Understanding on Rules and Procedures Governing the Settlement of Disputes), Aneks 2 k Marakeškemu sporazumu o ustanovitvi Svetovne trgovinske organizacije.

Postopek posvetovanj o sporih med državami je sicer poznal tudi GATT. Spore so obravnavali paneli, ki so imeli šibke pristojnosti izrekanja priporočil, h katerim so dale soglasje pogodbenice GATT in niso bila zavezujoča. Ob ustanovitvi WTO je prevladala ideja, da tak sistem za učinkovit razvoj mednarodne trgovine ne zadošča več.[173]

DSU je vzpostavil zapleten postopek za reševanje sporov (Dispute Settlement System, v nadaljevanju DSS), ki je sestavljen iz postopka za reševanje posameznih sporov pred paneli in postopka pred pritožbenim organom (Appellate Body). Postopek za reševanje sporov WTO pa ni popolnoma avtonomen, saj je podrejen DSB, ki je pravzaprav plenarni organ WTO – generalni svet, ki se sestaja kot DSB z ločenimi pristojnostmi. Ima številne funkcije, med drugim usmerja delo DSS, spremlja posvetovanja med državami članicami, ustanavlja panele, sprejema ali zavrača odločitve teles razsojanja in nadzira izpolnjevanje priporočil.[174]

Reševanje sporov v WTO se razlikuje od mnogih mednarodnopravnih režimov po tem, da članice vnaprej sprejmejo pristojnost razsojanja v okviru enkratnega prevzema obveznosti.[175] Glavna prednost tega sistema je, da lahko vsaka država članica WTO začne postopek proti katerikoli drugi članici na podlagi sporazuma WTO ali na podlagi kateregakoli drugega sporazuma WTO.

5.2.1 Razlogi za tožbo in vrste tožb

Članica WTO lahko zahteva začetek postopka za reševanje spora, če meni, da je v skladu s XXIII. členom GATT neposredno ali posredno izničena ali oškodovana njena pravica, ki ji pripada na podlagi sporazuma WTO in ne more doseči cilja, ki ga sporazum zagotavlja, je doseganje tega cilja ovirano, ali pa se je znašla v kakšni podobni situaciji.[176]

---

[173] Türk D., 2015, nav. delo, str. 389.

[174] Prav tam, str. 389–390; Peterlin I., nav. delo, str. 198–200.

[175] Prevzem obveznosti v paketu (pristop *single package*) od vseh držav zahteva enkratni prevzem obveznosti (*single undertaking*), kar pomeni da ob vključitvi v WTO sprejemejo tudi vse zajete večstranske sporazume, izjeme od tega pravila pa so izredno ozko določene. Peterlin I., nav. delo, str. 130.

[176] GATT, Article XXIII, Nullification or Impairment, dostopno na: https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art23_e.pdf (7. 10. 2016).

Sistem za reševanje sporov WTO pozna tri vrste tožb.[177] [178] S tožbami zaradi kršitev sporazumov WTO s strani druge pogodbenice (violation complaints) tožnik zatrjuje, da je ravnanje druge članice prizadelo ali omejijo njeno trgovino v nasprotju s sporazumom. V primeru take tožbe se domneva, da ima kršitev pravil škodljive učinke za druge članice pogodbenice sporazuma WTO, kar povzroči, da je dokazno breme, da ne gre za izničenje ali oškodovanje, na toženi stranki.[179] Druga vrsta tožb so tožbe zaradi nekršitev (non – violation complaints s katerimi tožeča država izpodbija ukrep, ki sicer ne pomeni kršitev določb sporazumov WTO, vendar pa spodkopava svobodno trgovino in ali ravnotežje vzajemnih zavez članic. DSU predvideva tudi situacijske tožbe (situation complaints), za vložitev katere zadostuje, da članica zatrjuje, da je v položaju v katerem ji je izničena ali zmanjšana ugodnost,[180] vendar pa ta tožba v praksi nikoli ni bila uporabljena.

5.2.2 Faze v postopku za reševanja spora

Reševanje spora v WTO ima tri faze: posvetovanja, panelni postopek in pritožbeni postopek. Posvetovanja so obvezna predhodna stopnja panelnega postopka in so lahko bilateralna ali multilateralna, glede na to ali v postopku sodelujeta le dve državi, ki sta v sporu ali pa kakšna tretja država izkaže, da ima bistven trgovinski interes in se zaradi tega želi vključiti v postopek posvetovanj.[181] Če stranki s posvetovanji v roku ne razrešita spora, lahko tožeča stranka poda zahtevo za ustanovitev panela,[182] o kateri odloči DSB in ustanovitev panela sprejme, razen če s konsenzom ne določi, da panela ne ustanovi.[183] Panel mora celovito in objektivno preučiti predloženo zadevo in ugotoviti skladnost z ustreznimi zajetimi sporazumi, pri tem pa mora obema strankama v sporu dati možnost, da navajata dejstva, ki omogočajo razjasnitev spora

[177] Angleško besedilo DSU uporablja izraz *complaint*, zaradi jasnosti bom za vlogo na prvi stopnji uporabila izraz tožba, ki je uporabljen tudi v slovenskem prevodu, vlogo v pritožbenem postopku pa bom imenovala pritožba. Enako terminologijo uporabi tudi *Peterlin*, v: Peterlin I., nav. delo, str. 206–208.

[178] Prvi odstavek XXIII. člena GATT.

[179] Osmi odstavek 3. člena DSU.

[180] Drugi odstavek 26. člena DSU.

[181] 4. člen DSU.

[182] Uradni slovenski prevod uporablja izraz ugotovitveni svet, vendar pa se v literaturi pogosteje uporablja izraz panel ali panelna skupina, zato bom tudi sama v magistrskem diplomskem delu uporabljala izraz panel.

[183] Prvi odstavek 6. člena DSU.

in preizkusiti njune navedbe.[184] V primeru multilateralnih sporov se ustanovi le en panel, kljub udeležbi večih strank, ki imajo bodisi položaj države tožnice,[185] bodisi le varujejo svoj bistveni interes v obravnavanem sporu, kljub temu, da nimajo vloge tožnice v postopku.[186] Poročila panela potem sprejme DSB,[187] razen če s konsenzom ne odloči o nasprotnem, če stranke tožbe ne umaknejo ali se na poročilo panela ne pritožijo. Katerakoli stranka v postopku ima pravico do pritožbe zoper poročilo panela, ki jo obravnava stalni pritožbeni organ, vendar pa je postopek pritožbe strogo omejen na pravna vprašanja in vprašanja pravne razlage. Pritožbeni organ lahko v tem omejenem obsegu potrdi, spremeni ali razveljavi poročilo panela.[188] Sledi potrjevanje v DSB, postopek je enak kot pri potrjevanju panelnih poročil. Odločitev DBS je za stranki spora zavezujoča.

Stranke v sporu imajo vedno na voljo tudi neformalne prostovoljne načine reševanja sporov, ki jih predvideva DSU.[189] Za razliko od posvetovanj niso obvezna faza reševanja spora in lahko potekajo v katerikoli fazi postopka, če o tem stranki skleneta dogovor.[190] Države članice WTO imajo za reševanje spora na voljo tudi posebno vrsto *ad hoc* arbitraže, ki jo ustanovijo na podlagi arbitražnega sporazuma in o kateri morajo obvestiti ostale članice WTO in DSB ali generalni svet.[191]

5.2.3 Nadzor nad implementacijo priporočila DSB

Zagotovitev učinkovitosti postopka za reševanje sporov WTO je v veliki meri odvisna od možnosti nadaljnjega ukrepanja organov WTO v primeru ugotovljene kršitve določb sporazuma WTO ali zajetih sporazumov. Država članica, ki je spor izgubila, mora v vnaprej predvidenem roku implementirati odločitev, tako da uskladi ravnanje s priporočili ali odločitvami DSB. Če kršiteljica svojega ravnanja ne uskladi, DSU predvideva dve obliki sankcij: kompenzacijo in kot skrajni ukrep se lahko proti državi

[184] Prvi in drugi odstavek 7. člena in 11. člen DSU.

[185] 9. člen DSU.

[186] 10. člen DSU.

[187] 16. člen DSU.

[188] Trinajsti odstavek 17. člena DSU.

[189] Prostovoljna sredstva za reševanje sporov so dobre usluge (*good offices*), sprava (*conciliation*) in posredovanje (*mediation*); ker so si v marsičem podobna, jih v praksi težko ločujemo, vsem pa je skupno, da lahko pripeljejo do pomiritve med strankama. Peterlin I., nav. delo, str. 201–202.

[190] 5. člen DSU.

[191] 25. člen DSU.

kršiteljici uporabi protiukrep[192], [193] vse z namenom čim prejšnje rešitve spora in vzpostavitve ravnovesja v mednarodni trgovini.

5.3 Pristojnost postopka za reševanje sporov WTO za odločanje o vprašanju ekonomskega kibernetskega vohunstva

Kljub temu, da vse države članice WTO avtomatično sprejmejo pristojnost razsojanja postopka za reševanje sporov WTO, pa lahko paneli in pritožbeni organ odločajo le o skladnosti ukrepov države s pravom WTO, torej sporazumom WTO in zajetimi sporazumi, [194] nimajo pa splošne pristojnosti za odločanje o tem, ali je morda kršeno kakšno drugo pravilo mednarodnega prava, na primer pravilo mednarodnega diplomatskega, okoljskega ali prava morja ali prava človekovih pravic.

Država, ki bi se odločila za uporabo mehanizma za reševanje sporov WTO zaradi ekonomskega kibernetskega vohunstva, bi tako lahko zatrjevala le kršitev obveznosti, ki izhaja iz prava WTO. Avtorji kot najbolj relevantno mednarodno pogodbo v normativnem okviru WTO za vprašanje ekonomskega kibernetskega vohunstva navajajo sporazum TRIPS, ki je bil sprejet na koncu urugvajskega kroga pogajanj leta 1995 in vsebuje temeljna mednarodna pravila o zaščiti pravic intelektualne lastnine. Posebnost sporazuma TRIPS je, da preko sklicevanja na določbe drugih mednarodnih sporazumov slednje vključuje v normativni sistem WTO, čeprav so sicer sprejete v okviru Svetovne organizacije za intelektualno lastnino (World Intelectial Property Organisation – WIPO). To so na primer nekatere določbe Bernske konvencije za varstvo književnih in umetniških del[195] in Pariške konvencije o zaščiti industrijske lastnine[196].

[192] Glede protiukrepov, ki sledijo neuskladitvi ravnanj v skladu s priporočilom DSB je treba zaradi terminološke jasnosti poudati, da gre za ukrepe, ki so primerljivi s protiukrepi, ki jih urejajo Pravila o odgovornosti držav za mednarodno protipravna dejanja, vendar jih ne smemo enačiti. Peterlin I., nav. delo, str. 220.

[193] Osmi odstavek 22. člena DSU.

[194] Prvi odstavek 1. člena DSU.

[195] Bernska konvencija za varstvo književnih in umetniških del (Berne Covnention for the Protection of the Literary and Artistic Works), Uradni list SFRJ – MP, št. 31/72, Uradni list RS – MP, št.9/92.

[196] Pariška konvencija o zaščiti industrijske lastnine (Paris Convention for the Protection of Industrial Property), Uradni list SFRJ – MP, št. 5/74, Uradni list RS – MP, št.9/92.

Sporazum TRIPS je nastal zaradi potrebe po ureditvi minimalnih standardov zaščite, ki jih mora zagotoviti vsaka država članica vsem fizičnim in pravnim osebam vseh drugih članic WTO. Pravila o zaščiti intelektualne lastnine so bila pred tem med državami izrazito različno urejena, kar je prispevalo k pogostim sporom med državami, zato so razvite države zahtevale in tudi dosegle, da je sporazum TRIPS uredil minimalno stopnjo zaščite. Na podlagi sporazuma države sprejmejo obveznost prilagoditi svojo notranjo zakonodajo skupnim mednarodnim standardom, ki jih določa TRIPS, poleg tega pa prevzamejo tudi dolžnost določenih aktivnih ukrepov proti zlorabi pravic intelektualne lastnine.[197]

5.3.1 Kršitev načela enake obravnave

TRIPS ne prepoveduje ekonomskega vohunjenja *per se*, vendar pa v več določbah zagotavlja zaščito pravic, ki jih takšno ravnanje ogroža. Eno takih je načelo nacionalne obravnave (načelo enake obravnave), ki je hkrati tudi eno osrednjih načel prava WTO.[198] Načelo enake obravnave je izraženo v 3. členu TRIPS in od vsake države članice zahteva, da glede varstva pravic intelektualne lastnine državljanom drugih držav članic zagotovi enake ugodnosti kot svojim lastnim državljanom.[199] Namen te določbe je prepovedati državam, da bi diskriminirale med domačimi in tujimi podjetji glede zagotavljanja in uresničevanja pravic intelektualne lastnine. Pridobivanje velike količine zaupnih podatkov tujih podjetij in njihovo posredovanje lastnim podjetjem z namenom doseganja ekonomske prednosti po mnenju nekaterih avtorjev pomeni kršitev načela enake obravnave, ker države domača podjetja obravnavajo ugodneje.[200]

5.3.2 Kršitev dolžnosti varovanja neobjavljenih informacij

Prav tako je za obravnavanje ekonomskega kibernetskega vohunstva pomemben 39. člen TRIPS, ki od držav zahteva, da varujejo neobjavljene informacije. Člen

[197] Parajon Skinner C., nav. delo, str. 1195; World Trade Organisation: Understanding the WTO, 2015, str. 39, dostopno na: https://www.wto.org/english/thewto_e/whatis_e/tif_e/understanding_e.pdf (12. 10. 2016).

[198] Načelo enake obravnave je vseboval že GATT in vsebujejo ga tudi številni drugi sporazumi WTO. Peterlin I., nav. delo, str. 249; Lotrionte C., nav. delo, str. 533.

[199] 3. člen TRIPS.

[200] Malawer S., nav. delo , str. 4; Parajon Skinner C., nav. delo, str. 1195.

zagotavlja varstvo tistih informacij, ki predstavljajo skrivnost, poleg tega imajo trgovinsko vrednost prav zato, ker so skrivnost in je oseba, ki ima nadzor nad temi informacijami storila vse za ohranitev informacij kot skrivnosti.[201] To pa so prav gotovo tiste informacije, na katere merijo dejanja ekonomskega kibernetskega vohunstva.[202] Drugi odstavek 39. člena določa, da morajo imeti fizične in pravne osebe možnost preprečiti, da se informacija, ki je zakonito pod njihovim nadzorom, brez njihovega privoljenja ne objavi ali da jo drugi pridobijo ali uporabijo brez njihovega privoljenja v nasprotju s pošteno trgovinsko prakso.[203] Za odločitev ali ekonomsko kibernetsko vohunstvo krši to določbo TRIPS je torej ključnega pomena, kako razumemo izraz poštena trgovinska praksa.[204]

TRIPS je mednarodna pogodba in kljub temu, da je vključena v normativni sistem WTO, se za njeno razlago uporabijo pravila razlage, ki jih določa Dunajska konvencija o pravu mednarodnih pogodb,[205] ki za izhodišče določa jezikovno razlago. Pogodbo je treba razlagati v dobri veri, po običajnem pomenu izrazov, uporabljenih v pogodbi v njihovem kontekstu ter luči njenega predmeta in cilja.[206]

Izraz poštena trgovinska praksa je potrebno razumeti v pomenu, v kakršnem se uporablja v okviru WTO in sporazuma TRIPS.[207] Podrobneje je izraz pojasnjen v opombi k 39. členu TRIPS, ki določa, da se za kršitev takšne prakse štejejo vsaj ravnanja, ki pomenijo kršitev pogodbe, kršitev zaupanja ali ravnanja, ki na takšno kršitev napeljujejo ter vsaka pridobitev informacije s strani oseb, ki so vedele ali zaradi velike malomarnosti niso vedele, da je bila informacija pridobljena z uporabo

[201] Drugi odstavek 39. člena TRIPS.

[202] Strawbridge J., nav. delo, str. 856–857.

[203] Drugi odstavek 39. člena TRIPS.

[204] Strawbridge J., nav. delo, str. 851; Veber M., nav. delo, str. 18.

[205] Glej npr. odločitev Pritožbenega organa v zadevi India - Patent Protection for Pharmaceutical and Agricultural Chemical Products, v katerem je navedeno: "These rules must be respected and applied in interpreting the TRIPS Agreement or any other covered agreement. ... Both panels and the Appellate Body must be guided by the rules of treaty interpretation set out in the Vienna Convention, and must not add to or diminish rights and obligations provided in the WTO Agreement." India - Patent Protection for Pharmaceutical and Agricultural Chemical Products, WT/DS50/AB/R, 1997, §46.

[206] Prvi odstavek 31. člena Dunajske konvencije o pravu mednarodnih pogodb (Vienna Convention on the Law of Treaties), Uradni list SFRJ – MP, št. 30/72, Uradni list RS – MP, št. 9/92.

[207] Türk D., 2015, nav. delo, str. 206.

teh prepovedanih praks.[208] Ker tudi v tej opombi ne najdemo zaključenega seznama vseh nepoštenih praks, temveč gre le za eksemplifikativno naštevanje tistih najbolj spornih, in tudi sicer pojem ni natančno definiran, je najbolje sprejeti stališče, da je pojem poštenosti potrebno razlagati v skladu z vrednotami družbe v določenem času.[209]

Iz pripravljalnih del 39. člena TRIPS je razvidno, da med primere, ki predstavljajo kršitev poštene trgovinske prakse namenoma ni vključena tudi kraja intelektualne lastnine in katerakoli oblika vohunstva, saj so bile države soglasne, da gre za tako očitno kršitev, da izrecna navedba med spornimi praksami ni potrebna.[210]

Zaključimo lahko, da ekonomsko kibernetsko vohunjenje nasprotuje pošteni trgovinski praksi, zato bi lahko države, ki so tarče ekonomskega vohunstva, poleg kršitve 3. člena zatrjevale tudi kršitev 39. člena TRIPS.[211] Postavlja pa se vprašanje, ali se zaradi teritorialne omejenosti sporazuma TRIPS zaščita nanaša tudi na ravnanje države na tujem teritoriju.[212]

5.3.3 Kršitev določb Pariške konvencije za varstvo industrijske lastnine

Nekateri avtorji zagovarjajo tudi idejo, da bi ekonomsko kibernetsko vohunjenje obravnavali kot dejanje nelojalne konkurence s sklicevanjem na določbe Pariške konvencije za varstvo industrijske lastnine.[213] Sporazum TRIPS se v 39. členu neposredno sklicuje na člen 10.bis Pariške konvencije, ki je na ta način postal del pravnega reda WTO, s tem pa lahko države zatrjujejo kršitve te konvencije tudi v okviru postopka za reševanje sporov WTO. 10.bis člen Pariške konvencije od držav zahteva, da zagotovijo učinkovito varstvo pred nelojalno konkurenco, ki je opredeljena kot vsako dejanje, ki nasprotuje poštenim običajem v industriji in

[208] 10. opomba k 39. členu TRIPS, dostopno na: https://www.wto.org/english/tratop_e/trips_e/t_agm3_e.htm#Footnote10 (16. 10. 2016).

[209] Correa C. M., Trade Related Aspects of Intellectual Property Rights: A Commentary on the TRIPS Agreement, Oxford University Press, New York, 2007, str. 371.

[210] Strawbridge J., nav. delo, str. 857.

[211] Parajon Skinner C., nav. delo, str. 1195; Lotrionte C., nav. delo, str. 527.

[212] Za več glej točko 5.5.

[213] Strawbridge J., nav. delo, str. 845; Lotrionte C., nav. delo, str. 490.

trgovini.[214] Avtorji, ki preučujejo domet te določbe, se ne strinjajo, ali se učinkovito varstvo pred nelojalno konkurenco nanaša le varstvo pred zavajanjem,[215] ali pa mora biti varstvo, ki naj ga zagotovi država širše in vključuje tudi zaščito poslovnih skrivnosti in drugih zaupnih podatkov podjetij. *Strawbridge* navaja, da tako jezikovna in s tem primarna razlaga besedila Pariške konvencije, kot tudi zgodovina člena 10.bis in kontekst pojma nelojalna konkurenca podpirata širšo obliko varstva, ki ga zagotavlja člen 10.bis. Obenem pa priznava, da bi morala država, ki bi želela pred organi razsojanja WTO zatrjevati kršitev tega člena, premagati številne ovire, da bi ji uspelo to določbo razlagati na način, ki prepoveduje ekonomsko kibernetsko vohunstvo. Predvsem ni jasno, ali 10.bis člen državam samo nalaga obveznost, da učinkovito preprečujejo nelojalno konkurenco na svojem teritoriju v okviru nacionalnega prava, ali pa je mogoča tudi razlaga, ki samim državam prepoveduje dejanja, ki nasprotujejo poštenim običajem v industriji in trgovini, v ta okvir pa spada tudi prepoved ekonomskega kibernetskega vohunjenja.[216]

5.3.4 Pomen drugih pravil mednarodnega prava za odločanje DSS

Čeprav organi razsojanja WTO ne morejo sprejeti odločitve, da je ukrep države članice kršil kakšno drugo pravilo mednarodnega prava, poleg norm vsebovanih v sporazumih WTO, pa to ne pomeni, da v postopku odločanja drugi viri mednarodnega prava nimajo nikakršne vloge. DSU ne določa tako kot Statut Meddržavnega sodišča [217] vseh virov prava, ki naj jih organi razsojanja WTO uporabijo pri izpolnjevanju svojih nalog, vendar pa se paneli in pritožbeni organ v številnih odločitvah sklicujejo tudi na pravila mednarodnega javnega prava. Vendar pa se tako mednarodno običajno pravo, kot tudi splošna pravna načela uporabljajo le v omejenem obsegu za zapolnjevanje pravnih praznin, nastalih v sporazumih WTO.[218] Izjemo predstavljajo pravila mednarodnega običajnega prava, ki se nanašajo na

[214] 10.bis člen Pariške konvencije o zaščiti industrijske lastnine.

[215] Ožjo interpretacijo zagovarja na primer *Wadlov*, v: Wadlow C., Regulatory Data Protection Under TRIPS Article 39(3) and Article 10bis of the Paris Convention: Is There a Doctor in the House?, dostopno na: https://works.bepress.com/christopher_wadlow/1/ (15. 10. 2016).

[216] Strawbridge J., nav. delo, str. 849–852, 855.

[217] Prvi odstavek 38. člena Statuta Meddržavnega sodišča.

[218] Peterlin I., str. 163-164. Za več o virih prava WTO glej npr. Pauwelyn J. Sources of International Trade Law: Mantras and Controversies at the World Trade Organization, dostopno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2834772 (3. 11 .2016); Palmeter D., Mavroidis P. C., The WTO Legal System: Sources of Law, Columbia University Academic Commons, dostopno na: https://academiccommons.columbia.edu/catalog/ac%3A192377 (3. 11. 2016).

razlago mednarodnih pogodb, ki na podlagi drugega odstavka 3. člena DSU uživajo poseben status in se uporabljajo kot glavni vir prava WTO.[219] Razlaga s pomočjo pravil in načel splošnega mednarodnega prava pa ne sme pripeljati do rezultatov *contra legem*, niti se ne sme uporabiti za razlago nedvoumnih določb prava WTO.[220]

5.4 Možnost vložitve zahtevka zaradi nekršitev

Tudi če ekonomsko kibernetsko vohunstvo ne krši nobene določbe TRIPS, nekateri mednarodni pravniki menijo, da bi država lahko začela postopek na podlagi tožbe zaradi nekršitev[221]. *Parajon Skinner* zatrjuje, da ravno ekonomsko kibernetsko vohunstvo predstavlja tako ravnanje, ki bi zahtevalo uporabo te vrste tožb.[222] Dejanja ekonomskega kibernetskega vohunstva pomenijo krajo velike količine zaupnih podatkov, zato je dejansko izničena ali zmanjšana pravica do varstva intelektualne lastnine, ki jo zagotavlja TRIPS in s tem onemogočeno doseganje njegovih ciljev.[223]

Ratio tožb zaradi nekršitev leži v odpravljanju neravnovesja, ki nastane, če država članica nima možnosti ukrepati proti drugi članici, ki s svojim ravnanjem ovira doseganje ciljev WTO ne da bi kršila izrecno normo WTO.[224] Če sprejmemo predpostavko, da pravila WTO ustvarjajo zaveze za države članice le na njihovem teritoriju,[225] ne pa tudi za ravnanje izven njega, potem dejanja ekonomskega kibernetskega vohunstva ne kršijo določb TRIPS. S tem pa je državam, ki so tarče ekonomskega kibernetskega vohunstva onemogočen dostop do mehanizma za reševanje sporov WTO. Vložitev tožbe zaradi nekršitev bi tem državam zagotovila možnost rešitve njihovega spora.

Kljub temu, da tudi TRIPS predvideva možnost vložitve tožbe zaradi nekršitev, pa so države sklenile moratorij glede te določbe TRIPS, ki velja že od sprejema tega

[219] Drugi odstavek 3. člena DSU.

[220] Lotrionte C., nav. delo, str. 533; Peterlin I., nav. delo, str. 163.

[221] Za več glej točko 5.2.1.

[222] Parajon Skinner C, nav. delo, str. 1202.

[223] Strawbridge J., nav. delo, str. 862; Parajon Skinner C, nav. delo, str. 1202.

[224] Legal Basis for Dispute, Types of complaints and required allegations in GATT 1994, Non-violation Complaint, dostopno na: https://www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c4s2p2_e.htm (11. 10. 2016).

[225] Za več glej točko 5.5.

sporazuma in je bil zadnjič podaljšan decembra 2015, veljal pa bo vsaj še do Ministrske konference leta 2017.[226] Prevladujoče stališče držav članic WTO je, da bi bilo potrebno popolnoma izključiti možnost tožb zaradi nekršitev v okviru sporazuma TRIPS ali vsaj še naprej podaljševati moratorij,[227] zato je malo verjetno, da bi v bližnji prihodnosti države sprejele nasprotno odločitev in tako odprle to pot za vložitev zahtevka zaradi ekonomskega kibernetskega vohunstva.[228]

5.5 (Ne)primernost mehanizma WTO za reševanje sporov zaradi ekonomskega kibernetskega vohunstva

Vse več držav članic WTO se zaveda, da so (potencialne) tarče ekonomskega kibernetskega vohunstva in se zato soočajo z negativnimi posledicami, ki jih ta škodljiva aktivnost povzroča njihovemu gospodarstvu. Zakaj torej do danes nobena država članica WTO ni začela postopka pred organom za reševanje sporov WTO proti domnevni državi kršiteljici? *Fidler*[229] odgovarja, da je razlog za tako neaktivnost v tem, da mehanizma WTO in TRIPS sploh nista primerna za reševanje vprašanja ekonomskega kibernetskega vohunstva, prvič, ker je veljavnost sporazuma TRIPS teritorialno omejena, in drugič, ker bi bilo težko vzpostaviti mednarodno odgovornost države za takšno ravnanje.

Pravila WTO ustvarjajo zaveze za države članice na njihovem teritoriju in ne nalagajo splošne zahteve po spoštovanju teh zahtev izven njihovega ozemlja. Vendar pa dejanja ekonomskega kibernetskega vohunstva izkoriščajo možnost oddaljenega dostopa do zaupnih informacij, ki se nahajajo na teritoriju druge države, zato se postavlja vprašanje, kako in ali bi sploh lahko države članice v takem primeru oblikovale zahtevek, za obravnavo katerega bi bil pristojen organ za reševanje sporov

[226] Ministerial Decision of 19 December 2015, WT/MIN(15)/41 — WT/L/976, Tenth Ministerial Conference, Nairobi, 2015, dostopno na: https://www.wto.org/english/thewto_e/minist_e/mc10_e/l976_e.htm (11. 10. 2016).

[227] TRIPS: 'Non-Violation' Complaints (Article 64.2), Background and the current situation, dostopno na: https://www.wto.org/english/tratop_e/trips_e/nonviolation_background_e.htm (11. 10. 2016).

[228] Strawbridge J., str. 863.

[229] Fidler D., Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage, dostopno na: https://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/ (11. 10. 2016). Z njim se strinja tudi *Ziolkowski*, v: Ziolkowski K., nav. delo, str. 434.

WTO in v njem zatrjevale kršitev pravil TRIPS.[230] Tej ozki razlagi odločno nasprotujejo drugi mednarodni pravniki, ki zatrjujejo, da je vsaj načelo enake obravnave, vsebovano v 3. členu TRIPS, kršeno v primeru ekonomskega kibernetskega vohunstva, ker se diskriminatorni učinki ne glede na kraj delovanja kažejo na ozemlju države, ki je to aktivnost izvajala,[231] preozka razlaga določb TRIPS pa bi tudi oteževala doseganje ciljev sporazuma, ki so zapisani v preambuli.[232]

Kot drugi razlog za neprimernost mehanizma WTO za reševanje sporov nastalih zaradi ekonomskega kibernetskega vohunstva *Fidler* navaja težave pri vzpostavljanju odgovornost države. Tudi če bi država uspela oblikovati zahtevek, ki bi ga obravnaval organ za reševanje sporov WTO, bi morala država ne le dokazati, da gre za kršitev mednarodne obveznosti, temveč tudi, da je ravnanje tej državi pripisljivo.[233] Ker se še nobeno mednarodno telo za reševanje sporov ni ukvarjalo z vprašanjem ekonomskega kibernetskega vohunstva, je vprašljivo, kako bi premagale problem pripisljivosti ravnanj v kibernetskem prostoru in ali bi se pri tem lahko oprle na ugotovitve podjetij, ki se ukvarjajo z zagotavljanjem računalniške varnosti.[234] Tudi ta argument ne prepriča. Spori predloženi v panelno odločanje mnogokrat vsebujejo tehnično zahtevna vprašanja, ki so bistvenega pomena za razumevanje spora in njegovo razrešitev, zato DSU določa, da se lahko paneli v takih primerih glede specifičnih tehničnih vidikov spora posvetujejo s strokovnjaki ali strokovnimi skupinami različnih strok in pridobijo njihovo mnenje.[235] Prav tako se paneli prav zaradi kompleksnosti sporov, ki se rešujejo v WTO vedno soočajo z velikimi količinami najrazličnejših dokazov.[236] Postopek za reševanje sporov WTO je torej prilagojen reševanju raznovrstnih in zahtevnih vprašanj[237] in zato primeren tudi za reševanje sporov nastalih zaradi ekonomskega kibernetskega vohunstva.

[230] Ziolkowski K., nav. delo, str. 434; Fidler D., 2013, nav. delo, str. 3.

[231] Malawer S., nav. delo, str. 5; Lotrionte C., nav. delo, str. 525.

[232] Parajon Skinner C, nav. delo, str. 1197.

[233] 1. in 2. člen Pravil o odgovornosti držav za mednarodno protipravna dejanja. Za več o problemu pripisljivosti za ravnanja v kibernetskem prostoru glej točko 4.3.

[234] Fidler D., 2013, nav. delo, str. 3.

[235] 13. člen DSU. Podrobneje pa sestavo in delovanje teh strokovnih skupin (*expert review groups*) ureja Dodatek 4 k sporazumu DSU.

[236] Pauwelyn ilustrativno opisuje, da so »paneli običajno poplavljeni z dokazi«. (»...WTO panels have been flooded with evidence.«. Pauwelyn J., Proof and Persuasion in WTO Dispute Settlement: Who Bears the Burden?, 1 Journal of International Economic Law 227, 1998, str. 227).

[237] Grando M. T., Evidence, Proof, and Fact-Finding in WTO Dispute Settlement, Oxford University Press, New York, 2009, str. 2–4.

6. ZAKLJUČEK

Če so takoj po razkritju Edwarda Snowdna dnevno časopisje zapolnjevali članki o sistematičnih kršitvah človekovih pravic v programih množičnega nadzora, ki so popolnoma zasenčili le nekaj mesecev mlajše razkritje Mandiantovega poročila o ekonomskem kibernetskem vohunstvu, se danes situacija spreminja. Svetovni mediji, pa tudi stroka, ne le pravna, temveč tudi obveščevalna in informacijska, temu problemu posvečajo vedno več pozornosti. Upad napadov na podjetja v ZDA takoj po sklenitvi prijateljskega dogovora s Kitajsko je sprva kazal na to, da se je trend naraščanja napadov ustavil, vendar pa so podjetja, ki se ukvarjajo z računalniško varnostjo kmalu ugotovila, da se je val predvsem kitajskega ekonomskega kibernetskega vohunstva le preusmeril – nove tarče so postale Rusija, Japonska, Južna Koreja in Indija.[238] Ekonomsko kibernetsko vohunstvo tako ni več omejeno na izoliran spor med Kitajsko in ZDA, ampak postaja globalni problem. Zakaj torej države, čeprav se zavedajo, kako veliko grožnjo predstavlja tovrstna dejavnost njihovemu gospodarstvu, ne kažejo prav velike želje po tem, da bi ta problem naslovile na mednarodni ravni?

Menim, da države vprašanja zakonitosti vohunstva *per se* nikoli ne bodo pripravljene urediti na mednarodni ravni. Vohunstvo uživa, ne glede na to ali to želimo priznati ali ne, poseben status v mednarodnih odnosih, če že ne tudi v mednarodnem pravu. Po sami definiciji je to skrivna dejavnost, iz tega pa izvira odpor držav, da bi se o tem vprašanju pogovarjale odkrito.

Državam, ki so tarče vohunstva, tako ostajata dve možnosti: bodisi bodo poskusile rešiti spor sodno, z vložitvijo zahtevka zaradi kršitev veljavnih pravil mednarodnega prava na Meddržavno sodišče ali postopek reševanja sporov WTO, bodisi bodo ubrale diplomatsko pot in še naprej sklepale prijateljske sporazume v upanju, da se bo nasprotna stran pod grožnjo ekonomskih sankcij zavez držala.

Predvsem možnost reševanja spora nastalega zaradi dejavnosti ekonomskega kibernetskega vohunstva pred Meddržavnim sodiščem se mi zdi izredno malo

[238] Chinese Economic Cyber-Espionage Plummets in U.S.: Experts, dostopno na: http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D (18. 10. 2016).

verjetna, ker se države nerade spuščajo v spore, katerih končna odločitev je tako negotova kot v tem primeru. Čeprav je Meddržavno sodišče že večkrat odločalo o kršitvah načela ozemeljske suverenosti in načela neintervencije, se je situacija temeljito spremenila s pojavom kibernetskega prostora in nemogoče je napovedati, kako bi temeljna načela, ki so nastala v nekem popolnoma drugačnem času in okoliščinah, danes razlagalo to sodišče. Na tem mestu naj opozorim še na eno pomanjkljivost, zaradi katere menim, da Meddržavno sodišče ni najprimernejši forum za reševanje spora zaradi ekonomskega kibernetskega vohunstva. V zadnjih letih je Meddržavno sodišče odločalo o dveh kompleksnejših sporih[239], v katerih je bila končna odločitev o skladnosti ravnanja države z mednarodnim pravom v veliki meri odvisna od predhodnih znanstvenih in tehničnih ugotovitev. V obeh primerih se je (na žalost) izkazalo, da tako kompleksnim vprašanjem sodišče enostavno ni kos, na kar so opozorili tudi nekateri sodniki v svojih ločenih mnenjih. Predvsem vprašanja o pripisljivosti dejanj izvršenih v kibernetskem prostoru državi pa se ne da rešiti le na podlagi pravil mednarodnega prava, temveč ob pomoči poglobljene analize računalniške forenzike in drugih strokovnjakov. Dokler Meddržavno sodišče ne sprejme pomoči strokovnjakov, ki so relevantni za odločitev v določenem sporu, bo njihova odločitev skoraj zagotovo pomanjkljiva.[240] Kot sta zapisala sodnika Simma in Al-Khasawneh:

"Naloga sodišča ni znanstvena ocena tega, kar se je dejansko zgodilo, temveč presoja zahtevkov strank in ocena, ali so zahtevki dovolj utemeljeni, da pomenijo kršitev mednarodne obveznosti."[241]

Na drugi strani je postopek za reševanje sporov WTO prilagojen reševanju prav takih, tehnično zahtevnih sporov. Možnost ustanovitve posebne strokovne skupine, ni le potencialna možnost, ki jo imajo telesa razsojanja na voljo, temveč paneli in

[239] V mislih imam primer *Obratov celuloze na reki Urugvaj* iz leta 2010 in primer *Kitolova na Anktarktiki* iz leta 2014. Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgement, [2010] I.C.J. Rep.14; Whaling in the Antarctic (Australia v. Japan: New Zealand intervening), [2014] I.C.J. Rep.226.

[240] Za več o tem glej npr. Sandoval Coustasse J.G., Samuelsen E., Adjudicating Conflicts Over Resources: The ICJ's Treatment of Technical Evidence in the Pulp Mills Case, 3 Goettingen Journal of International Law 447, 2011. (...Probably the most controversial point of the decision, as highlighted by different judges in their dissenting and separate opinions and declarations, is how the Court established the facts of the case to make the determination that Uruguay was not in breach of its substantive obligations,...).

[241] Pulp Mills on the River Uruguay (Argentina v. Uruguay), Joint Dissenting Opinion of Judges Al-Khasawneh and Simma, [2010] I.C.J. Rep.108, §4.

pritožbeni organ to možnost tudi pogosto uporabijo. Vseeno pa bi država, ki bi zatrjevala kršitev sporazuma TRIPS zaradi ekonomskega kibernetskega vohunstva morala rešiti vprašanje teritorialne veljavnosti sporazuma, zato bi bila tudi odločitev v tem postopku izrazito nepredvidljiva. Poleg tega ne smemo pozabiti, da je namen postopka za reševanje sporov WTO reševanje trgovinskih sporov, medtem ko gre pri ekonomskem kibernetskem vohunstvu za širše vprašanje. Zato bo v prihodnje posebno pozornost potrebno nameniti predvsem temu, da postopek za reševanje sporov ne bo presegel svojih pristojnosti.

Kljub tej negotovosti pa nam lahko dokončen odgovor na vprašanje, ali ekonomsko kibernetsko vohunstvo krši mednarodno pravo, da samo odločitev sodišča ali pa sklenitev posebne mednarodne pogodbe, ki bi pogodbenicam prepovedovala tovrstno škodljivo dejavnost. Glede na to, da smo priča vedno pogostejšim diplomatskim, političnim in tudi pravnim nasprotovanjem ekonomskemu kibernetskemu vohunstvu, lahko morda pričakujemo vsaj, da bodo države nadaljevale s sklepanjem prijateljskih sporazumov, s katerimi se bodo zavezale, da ne bodo niti izvajale niti podpirale ekonomskega kibernetskega vohunstva. Ne moremo pa izključiti niti možnosti, da bi se države vendarle sporazumele o začetku pogajanj o celovitejši obravnavi delovanja držav v kibernetskem prostoru v okviru OZN.

Konec koncev, *v znanju je moč*. In države te moči ne bodo zlahka izpustile iz svojih rok.

7. VIRI

7.1 Monografske publikacije

1. Baslar K., The Concept of the Common Heritage of Mankind in International Law, Kluwer Law International, The Hague, 1998.
2. Bernik I., Prislan K., Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem, Fakulteta za varnostne vede, Univerza v Mariboru, Ljubljana, 2012.
3. Bogdandy A., Rüdinger W. (ed.), Max Planck Yearbook of United Nations Law, Volume 10, Brill Nijhoff, The Hague, 2006.
4. Correa C.M., Trade Related Aspects of Intellectual Property Rights: A Commentary on the TRIPS Agreement, Oxford University Press, New York, 2007.
5. Czosseck C., Ottis R., Ziolkowski K. (ed.), 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Talin, 2012.
6. Grando M.T., Evidence, Proof, and Fact-Finding in WTO Dispute Settlement, Oxford University Press, New York, 2009.
7. Ohlin J.D., Govern K., Finkelstein C. (ed)., Cyber War, Law and Ethic for Virtual Conflicts, Oxford University Press, Oxford, 2015.
8. Oppenheim L., International Law, A Treatise, Longman, Greens & Co., London, 1905.
9. Osula A., Rõigas H. (ed.), International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications, Talin, 2016.
10. Peterlin I., Svetovna trgovinska organizacija in državna suverenost, GV Založba, Ljubljana, 2013.
11. Roscini M., Cyber Operations and the Use of Force in International Law, Oxford University Press, New York, 2014.
12. Simma B., Khan D.E., Nolte G., Paulus A. (ed.), The Charter of the United Nations: A Commentary, Volume I, Oxford University Press, Oxford, 2012.
13. Shackelford S.J., Managing Cyber Attacks in International Law, Business, and Relations: in Search of Cyber Peace, Cambridge University Press, New York, 2014.
14. Toffler A., Powershift: knowledge, wealth and violence at the edge of the 21st century, Bantam Books, New York, 1991.
15. Tsagourias N., Buchan R., Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, Cheltenham, 2015.
16. Türk D., Načelo neintervencije v mednarodnih odnosih in v mednarodnem pravu, Mladinska knjiga, Ljubljana, 1984.
17. Türk D., Temelji mednarodnega prava, IUS Software, GV Založba, Ljubljana, 2015.
18. Završnik A., Kibernetska kriminaliteta, IUS SOFTWARE, GV Založba, Inštitut za kriminologijo pri Pravni fakulteti, Ljubljana, 2015.

19. Ziolkowski K. (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Talin, 2013.

7.2 Periodika

20. Allan C.S., Attribution Issues in Cyberspace, 13 Chicago-Kent Journal of International and Comparative Law 55, 2013, str. 55–83.
21. Baker C.D., Tolerance of International Espionage: A Functional Approach, 19 American University International Law Review 1091, 2003, str. 1091–1113.
22. Benatar M., The Use of Cyber Force: Need for Legal Justification?, 1 Goettingen Journal of International Law 375, 2009, str. 375–396.
23. Bomse A.L., The Dependence of Cyberspace, 50 Duke Law Review 1717, 2001, str. 1717–1749.
24. Bowett D.W., Economic Coercion and Reprisals by States, 13 Virginia Journal of International Law 1, 1972, str, 1–12.
25. Brown G., Poellet K., The Customary International Law of Cyberspace, 6 Strategic Studies Quarterly 126, 2012, str. 126–145.
26. Buchan R., Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?, 17 Journal of Conflict & Security Law 211, 2012, str. 211–225.
27. Chesterman S., The Spy Who Came in from the Cold War: Intelligence and International Law, 27 Michigan Journal of International Law 1071, 2006, str. 1071–1130.
28. Danielson M.E.A., Economic Espionage: A Framework for a Workable Solution, 10 Minnesota Journal of Law, Science & Technology 503, 2009, str. 503–-548.
29. Deeks A., An International Legal Framework for Surveillance, 55 Virginia Journal of International Law 291, 2014, str. 291–368.
30. Delupis I., Foreign Warships and Immunity for Espionage, 78 American Journal of International Law 53, 1984, str. 53–75.
31. Forcese C., Spies Without Borders: International Law and Intelligence Collection , 5 Journal of National Security Law & Policy 179, 2011, str. 179–210.
32. Forcese C., Pragmatism and Principle: Intelligence Agencies and International Law, 102 Virginia Law Review 67, 2016, str. 67–84.
33. Garcia Mora M.R., Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition, 26 University of Pittsburgh Law Review 65, 1964, str. 65–97.
34. Jamnejad M., Wood M., The Principle of Non-Intervention, 22 Leiden Journal of International Law 345, 2009, str. 345–381.
35. Johnson D, Post D., Law and Borders: The Rise of Law in Cyberspace, 48 Stanford Law Review 1367, 1996, str. 1367–1402.
36. Kunig P., Max Planck Encyclopedia of Public International Law, Prohibition of Intervention.

37. Lillich R.B., The Status of Economic Coercion Under International Law: United Nations Norms, 12 Texas International Law Journal 17, 1977, str. 17–23.
38. Lotrionte C., Countering State-Sponsored Cyber Economic Espionage Under International Law, 40 North Carolina Journal of International Law 443, 2015, str. 443–541.
39. Malawer S., Chinese Economic Cyber Espionage, U.S. Litigation in the WTO and Other Diplomatic Remedies, Georgetown Journal of International Affairs, 2015, str. 1–8.
40. Mattessich W., Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage, 54 Columbia Journal of Transnational Law 873, 2016, str. 873–896.
41. McDougal M.S., Lasswell H.D., Reisman W.M., The Intelligence Function and World Public Order, 46 Faculty Scholarship Series 365, 1973, str. 365–448.
42. Pauwelyn J., Proof and Persuasion in WTO Dispute Settlement: Who Bears the Burden?, 1 Journal of International Economic Law 227, 1998, str. 227–258.
43. Post D., What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace, 52 Stanford Law Review 1439, 2000, str. 1439–1459.
44. Radsan J.A., The Unresolved Equation of Espionage and International Law, 28 Michigan Journal of International Law 595, 2007, str. 595–623.
45. Rid T., Buchanan B., Attributing Cyber Attacks, 38 Journal of Strategic Studies 4, 2014, str. 4–37.
46. Sancin V., Odgovornost državnih organov za kršitve mednarodnega prava, Javna uprava, 2007, letnik 43, številka 2, str. 501–521.
47. Sandoval Coustasse J.G., Samuelsen E., Adjudicating Conflicts Over Resources: The ICJ's Treatment of Technical Evidence in the Pulp Mills Case, 3 Goettingen Journal of International Law 447, 2011, str. 447–471.
48. Schmitt M.N., Vihul L., Proxy Wars in Cyber Space: The Evolving International Law of Attribution, 1 Fletcher Security Review 55, 2014, str. 55–73.
49. Scott R.D., Territorially Intrusive Intelligence Collection and International Law, 46 Air Force Law Review 217, 1999, str. 217–226.
50. Sepura K., Economic Espionage: The Front Line of a New Economic War, 26 Syracuse Journal of International Law and Commerce 127, 1998, str. 127–150.
51. Shamsi J.A., Zeadally S., Sheikh F., Flowers A., Attribution in Cyberspace: Techniques and Legal Implications, 9 Security and Communications Network 2886, 2016, str. 2886–2900.
52. Stockburger P.Z., Known Unknowns: State Cyber Operations, Cyber Warfare, and the *Jus Ad Bellum*, 31 American University International Law Review 545, 2016, str. 545–591.
53. Strawbridge J., The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation, 47 Georgetown Journal of International Law 833, 2016, str. 833–863.
54. Tucker D., The Federal Government's War on Economic Espionage, 18 Journal of International Law 1109, 2014, str. 1109–1152.

55. Veber M., Ali kibernetski prostor spreminja mednarodnopravne vidike ekonomskega vohunstva med državami? Pravna praksa, letnik 2016, številka 10, str. 16–18.
56. Yoo J., Sulmasy G., Counterintuative: Intelligence Operations and International Law, 28 Michigan Journal of International Law 625, 2006, str. 625–638.
57. Ziegler K.S., Max Planck Encyclopedia of Public International Law, *Domain Réservé.*

7.3 Mednarodne pogodbe

58. Bernska konvencija za varstvo književnih in umetniških del (Berne Covnention for the Protection of the Literary and Artistic Works), Uradni list SFRJ – MP, št. 31/72, Uradni list RS – MP, št.9/92.
59. Dunajska konvencija o pravu mednarodnih pogodb (Vienna Convention on the Law of Treaties), Uradni list SFRJ – MP, št. 30/72, Uradni list RS – MP, št. 9/92.
60. Marakeški sporazum o ustanovitvi Svetovne trgovinske organizacije (Marakesh Agreement – Agreement Establishing the World Trade Organisation), Uradni list RS – MP, št.10/95.
61. Pariška konvencija o zaščiti industrijske lastnine (Paris Convention for the Protection of Industrial Property), Uradni list SFRJ – MP, št. 5/74, Uradni list RS – MP, št.9/92.
62. Splošni sporazum o carinah in trgovini (General Agreement on Tariffs and Trade 1947), Uradni list RS – MP, št. 4/94.
63. Sporazum o trgovinskih vidikih pravic intelektualne lastnine (Agreement on Trade – Related Intelectual Property Rights), Uradni list RS – MP, št.10/95.
64. Ustanovna listina OZN (Charter of the United Nations), Uradni list RS –MP, št.1/14.

7.4 Nacionalna zakonodaja

65. Economic Espionage Act, Pub.L. 104-294, 110 Stat. 3488, enacted October 11, 1996, dostopno na: https://www.gpo.gov/fdsys/pkg/PLAW-104publ294/html/PLAW-104publ294.htm (30. 9. 2016).

7.5 Judikatura

66. Armed Activities on the Territory of Congo (Democratic Republic of Congo v. Uganda), Judgment, [2005] I.C.J.Rep.168.
67. Case of the S.S. "Lotus" (France v. Turkey), [1927], P.C.I.J. (Ser.A)No.10.

68. Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), Merits, [1949] I.C.J. Rep.4.
69. Case Concerning Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium), Joint Separate Opinion of Judges Higgins, Kooijmans and Buergenthal, [2002] I.C.J. Rep.63.
70. Island of Palmas Case (Netherlands v. United States of America), RIAA, Vol. II, str. 838.
71. India - Patent Protection for Pharmaceutical and Agricultural Chemical Products, WT/DS50/AB/R, 1997.
72. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, [1996], I.C.J. Rep.226
73. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA), Merits, [1986] I.C.J. Rep.14.
74. Nationality Decrees Issued in Tunis and Morocco, Advisory Opinion, [1923], P.C.I.J. (Ser.B)No.4.
75. North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands), [1969] I.C.J. Rep.3.
76. Oil Platforms (Islamic Republic of Iran v. United States of America), Separate Opinion of Judge Buergenthal, [2003] I.C.J.Rep.270.
77. Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Provisional Measures, [2014] I.C.J. Rep.147.
78. United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), [1980], I.C.J.Rep.3.
79. Pulp Mills on the River Uruguay (Argentina v. Uruguay), Joint Dissenting Opinion of Judges Al-Khasawneh and Simma, [2010] I.C.J. Rep.108.
80. Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgement, [2010] I.C.J. Rep.14.
81. Whaling in the Antarctic (Australia v. Japan: New Zealand intervening), [2014] I.C.J. Rep.226.

7.6 Dokumenti OZN in WTO

82. Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, GA OR, 56th Sess., UN Doc. A/RES/56/83.

83. Deklaracija načel mednarodnega prava o prijateljskih odnosih in sodelovanju med državami v skladu z ustanovno listino OZN (Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations), Resolucija Generalne Skupščine OZN, 2625(XXV), UN Doc. A/RES/25/2625, 1970.

84. Deklaracija o nedopustnosti intervencije in vmešavanja v notranje zadeve držav (Declaration on the Inadmissibility of Intervention and Interference in the Internal

Affairs of the States), Resolucija Generalne Skupščine OZN, UN Doc. A/RES/36/103, 1981.

85. Deklaracija o nedopustnosti intervencije v notranje zadeve držav in o zaščiti njihove neodvisnosti in suverenosti (Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, Resolucija Generalne Skupščine OZN, 2131(XX), UN Doc. A/RES/20/2131, 1965.
86. Letter dated 6 September 2012 from the Chargé d'affaires a.i. of the Permanent Mission of Azerbaijan to the United Nations addressed to the Secretary-General, UN Doc. A/66/897-S/2012/687.
87. Ministerial Decision of 19 December 2015, WT/MIN(15)/41 — WT/L/976, Tenth Ministerial Conference, Nairobi, 2015, dostopno na: https://www.wto.org/english/thewto_e/minist_e/mc10_e/l976_e.htm (11. 10. 2016).
88. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24. 6. 2013.
89. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22. 7. 2015.
90. Second Report on the Identification of Customary International Law, International Law Commission UN Doc. A/CN.4/672, 22. 5. 2014.

7.7 Spletni članki

91. Fidler D., Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies, American Society of International Law, Insights 17, 2013.
92. Fidler D., U.S.-China Cyber Deal Takes Norm Against Economic Espionage Global, dostopno na: http://blogs.cfr.org/cyber/2015/09/28/u-s-china-cyber-deal-takes-norm-against-economic-espionage-global/ (30. 9. 2016).
93. Fidler D., Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage, dostopno na: https://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/ (11. 10. 2016).
94. Merkin K., Critical Analysis: Economic Espionage and International Law, dostopno na: http://djilp.org/4721/critical-analysis-economic-espionage-and-international-law/ (4. 10. 2016).
95. Not so Secret: Deal at the Heart of UK-US Intelligence, dostopno na: https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released (30. 9. 2016).

96. Palmeter D., Mavroidis P.C., The WTO Legal System: Sources of Law, Columbia University Academic Commons, dostopno na: https://academiccommons.columbia.edu/catalog/ac%3A192377 (3. 11. 2016).
97. Pauwelyn J. Sources of International Trade Law: Mantras and Controversies at the World Trade Organization, dostopno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2834772 (3. 11. 2016).
98. Sastry S.S., The Newton-Leibniz Controversy over the Invention of the Calculus, dostopno na: http://pages.cs.wisc.edu/~sastry/hs323/calculus.pdf (30. 9. 2016).
99. The Latest on Chinese-Affiliated Intrusions into Commercial Companies, dostopno na: https://www.crowdstrike.com/blog/the-latest-on-chinese-affiliated-intrusions-into-commercial-companies/ (30. 9. 2016).
100. U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict, dostopno na: http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html (3. 11. 2016).
101. Wadlow C., Regulatory Data Protection Under TRIPS Article 39(3) and Article 10bis of the Paris Convention: Is There a Doctor in the House?, dostopno na: https://works.bepress.com/christopher_wadlow/1/ (15. 10. 2016).
102. World Trade Organisation: Understanding the WTO, 2015, dostopno na: https://www.wto.org/english/thewto_e/whatis_e/tif_e/understanding_e.pdf (12. 10. 2016).

7.8 Drugi viri

103. American Enterprise Institute: Cybersecurity and American Power, Addresing New Threats to America's Economy and Military, Keynote Address, Gen. Keith B. Alexander, dostopno na: https://www.aei.org/events/cybersecurity-and-american-power/ (30. 9. 2016).
104. Barlow J.P., A Declaration of Independence for Cyberspace, dostopno na: https://www.eff.org/cyberspace-independence (3. 10. 2016).
105. Bibliotekarska terminologija: Koliko je en kilobajt, megabajt, gigabajt?, dostopno na: http://terminologija.blogspot.si/2010/11/koliko-je-en-kilobajt-megabajt-gigabajt.html (18. 10. 2016).
106. Brazilian President: US Surveillance a »Breach of International Law«, dostopno na: https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance (3. 10. 2016).
107. Brief History of Internet, dostopno na: http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf (3. 10. 2016).
108. China Working to Halt Commercial Cyberwar in Deal with Germany, dostopno na: http://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany (1. 10. 2016).

109. Chinese Economic Cyber-Espionage Plummets in U.S.: Experts, dostopno na: http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D (18. 10. 2016).
110. CrowdStrike Intelligence Report, Putter Panda, dostopno na: https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf (1. 11. 2016).
111. Cyberwar and Sony, dostopno na: http://blogs.law.unc.edu/ncilj/2015/01/21/cyberwar-and-sony/ (3. 10. 2016).
112. Department of Defense, Dictionary of Military Terms, »Cyberspace«, dostopno na: http://www.dtic.mil/doctrine/dod_dictionary/ (3. 10. 2016).
113. FBI Audio, Donfan "Greg" Chun, dostopno na: https://www.fbi.gov/audio-repository/news-podcasts-gotcha-dongfan-greg-chung.mp3/view (18.10.2016).
114. FireEye Special Report: Red Line Drawn, China Recalculates its Use of Cyber Espionage, dostopno na: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf (1. 10. 2016).
115. Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, okrober 2011, dostopno na: https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (18. 10. 2016).
116. Fran, Slovarji Inštituta za slovenski jezik Frana Ramovša ZRC SAZU, Slovar slovenskega knjižnega jezika, geslo: vohuniti, dostopno na: http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=vohuniti&hs=1 (1. 11.2016).
117. GATT, Article XXIII, Nullification or impairment, dostopno na: https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art23_e.pdf (7.10.2016).
118. G20 Leaders' Communique, Antalya Summit, november 2015, dostopno na: http://www.consilium.europa.eu/en/press/press-releases/2015/11/16-g20-summit-antalya-communique/ (1. 10. 2016).
119. Kranjc M., Pripisljivost ravnanj izvršenih na podlagi navodil ali usmeritev in nadzora države, diplomsko delo, Ljubljana 2014.
120. Lewis J.A., The Cyber War has Not Begun, Center for Strategic and International Studies, 2010, str.2, dostopno na: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100311_TheCyberWarHasNotBegun.pdf (4. 10. 2016).
121. Lowenfeld A.F., Breton Woods Conference (1944), Max Planck Encyclopedia of Public International Law.
122. Mandiant, APT 1: Exposing One of China's Cyber Espionage Units, dostopno na: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (30. 9. 2016).
123. More Sanctions on North Korea after Sony Case, dostopno na: http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html?_r=0 (3. 10. 2016).

124. Obama Order Sped Up Wave of Cyberattacks Against Iranhttp://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=3&pagewanted=1&pagewanted=all (9. 11. 2016).
125. The U.S. and China Agree Not to Conduct Economic Espionage in Cyberspace, dostopno na: https://www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html (19. 10. 2016).
126. The White House, Office of the Press Secretary, september 2015: Fact Sheet: President Xi Jinping's State Visit to the United States, dostopno na: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (30. 9. 2016).
127. TRIPS: 'Non-Violation' Complaints (Article 64.2), Background and the current situation, dostopno na: https://www.wto.org/english/tratop_e/trips_e/nonviolation_background_e.htm (11. 10. 2016).
128. UKUSA Agreement Release 1940–1956, dostopno na: https://www.nsa.gov/news-features/declassified-documents/ukusa/ (30. 9. 2016).
129. U.S. Ambassador Baucus says China hacking threatens national security, dostopno na: http://www.reuters.com/article/us-china-usa-baucus-idUSKBN0F00S320140625.
130. U.S. Department of Defense, The Strategy for Homeland Defense and Civil Support, 2005, dostopno na: http://www.wslfweb.org/docs/usg/homeland.pdf (3. 10. 2016).
131. Understanding the WTO, Who we are?, dostopno na: https://www.wto.org/english/thewto_e/whatis_e/who_we_are_e.htm (7. 10. 2016).
132. Understanding the WTO: What is the World Trade Organization?, dostopno na: https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact1_e.htm (7. 10. 2016).
133. United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui, Indictment, United States District Court, Western District of Pennsylvania, dostopno na: https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf (30. 9. 2016).
134. What are the Best Mini USB 3.0 USB Drives?, dostopno na: http://www.everythingusb.com/mini-drives.html (18. 10. 2016).
135. Xi Jinping State Visit: UK and China Sign Cybersecurity Pact, dostopno na: https://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron (1. 10. 2016).