Primjena međunarodnog humanitarnog prava na kibernetičke napade

Kruljac, Dario

Pravni fakultet Sveučilišta u Zagrebu

Katedra za međunarodno pravo

Dario Kruljac

PRIMJENA MEĐUNARODNOG HUMANITARNOG PRAVA NA KIBERNETIČKE NAPADE

DIPLOMSKI RAD

Mentorica: prof.dr.sc. Maja Seršić

Zagreb, listopad 2023.

Izjava o izvornosti

Ja, Dario Kruljac, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključiv autor diplomskog rada te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristio drugim izvorima od onih navedenih u radu.

Dario Kruljac, v.r.

Sažetak:

Sve učestaliji kibernetički napadi i njihovo korištenje u oružanim sukobima 21. stoljeća otvorili su novu domenu ratovanja - kibernetički prostor. Zbog velike međupovezanosti civilnih i vojnih sustava u kibernetičkom prostoru, vrlo je teško provoditi kibernetičke napade u skladu s glavnim ciljem i svrhom međunarodnog humanitarnog prava - zaštitom civila i civilnih objekata. Štoviše, upitno je mogu li se pravila, načela i terminologija međunarodnog humanitarnog prava, nastala uzimajući u obzir potpuno drugačiju vrstu ratovanja, primijeniti na kibernetičke napade. Zato će prvi dio ovog rada pojasniti može li se međunarodno humanitarno pravo primijeniti na kibernetičke operacije. S obzirom na specifičnosti kibernetičkih napada, odnosno činjenica da se ne provode uporabom kinetičke sile, da se provode u virtualnom prostoru gdje istovremeno djeluje velik broj ljudi te da infrastruktura toga prostora ima i civilnu i vojnu namjenu, može doći do poteškoća u primjeni tradicionalnih pravila međunarodnog humanitarnog prava o vođenju neprijateljstava. Zbog toga će naglasak drugog dijela rada biti na primjeni pravila međunarodnog humanitarnog prava, posebice pravila razlikovanja, proporcionalnosti i mjera opreza, na kibernetičke napade.

Ključne riječi: kibernetički napadi, kibernetičko ratovanje, međunarodno humanitarno pravo pravilo razlikovanja, pravilo proporcionalnosti, mjere opreza

Summary:

Increasingly frequent cyberattacks and their use in armed conflicts of the 21st century have opened up a new domain of warfare - cyberspace. Due to the large interconnection of civil and military systems in cyberspace, it is very difficult to carry out cyber attacks in accordance with the main aim and purpose of international humanitarian law - the protection of civilians and civilian objects. Moreover, it is questionable whether the rules, principles and terminology of international humanitarian law, created by taking into account a completely different type of warfare, can be applied to cyber attacks. That is why the first part of this paper will clarify whether international humanitarian law can be applied to cyber operations. Given the specifics of cyber attacks, i.e. the fact that they are not carried out using kinetic force, that they are carried out in a virtual space where a large number of people operate at the same time, and that the infrastructure of that space has both civilian and military purposes, there may be difficulties in the application of traditional rules of international humanitarian law on the conduct of hostilities. For this reason, the emphasis of the second part of the paper will be the application of the rules of international humanitarian law, especially the rules of distinction, proportionality and precautions, to cyberattacks.

Keywords: cyberattacks, cyber warfare, international humanitarian law, principle of distinction, principle of proportionality, principle of precautions

Sadržaj

1. UVOD

"*Dobro je što je rat tako užasan, inače bismo ga previše zavoljeli*" - rekao je general vojske Konfederacije Robert E. Lee u bitci kod Fredericksburga.[1] I doista, od najranijih vremena ljudi su pribjegavali ratu kao načinu širenja teritorija, rješavanja sporova ili samo zbog puke potrebe za nasiljem. Ipak, gledajući sve strahote koje rat može donijeti, ubrzo je postalo jasno kako su potrebna određena ograničenja vođenja sukoba. Već vrlo rano u razvoju čovječanstva mogu se pronaći stanovita pravila ratovanja. U starom Egiptu, Babilonu i Indiji, bilo je zabranjeno koristiti skriveno ili otrovno oružje, te napadati neprijateljske snage koje su se predale, bježe ili su položile svoje oružje.[2] U gradovima-državama antičke Grčke hramovi, svećenici i veleposlanstva smatrani su nepovredivima, a smatralo se pogrešnim onemogućiti neprijatelju opskrbu pitkom vodom.[3] U srednjem vijeku, na Drugom lateranskom koncilu 1139. godine osuđena je upotreba samostrela.[4] Lieber code iz 1863. godine, objavljen manje od godinu dana nakon već spomenute bitke kod Fredericksburga, uređuje ponašanje u ratu vojske Unije i ujedno predstavlja prvi pokušaj kodificiranja ratnih zakona te između ostalog navodi da "*vojna nužda ne dopušta okrutnost - to jest, nanošenje patnje samo radi patnje ili osvet*e"[5] te da "*nenaoružani građanin treba biti pošteđen osobno, kao i njegova imovina i čast onoliko koliko to ratne potrebe dopuštaju*".[6]

Daljnjim napretkom znanosti i tehnologije pojavila su se nova oružja čiji je učinak znatno povećao okrutnost ratovanja. Zato su države nastojale zaključiti sporazume koji će ograničiti takva oružja.[7] Uskoro je kao glavna svrha međunarodnog prava oružanih sukoba prepoznata potreba otklanjanja okrutnosti, sprječavanja strašnih oblika vođenja borbe, te zaštita civila i civilne imovine.[8] U tu svrhu zaključene su Ženevska konvencija iz 1864. godine, Haške

[1] Blount, Roy, Making Sense of Robert E. Lee, Smithsonian Magazine, 2003, Dostupno na: https://www.smithsonianmag.com/history/making-sense-of-robert-e-lee-85017563/ (26.9.2023.)
[2] Hongsheng, Sheng, "The Evolution of the Law of War", Chinese Journal of International Politics, Vol 1/2006, str. 272.
[3] Green, Leslie, C., "The Law of War in Historical Perspective", International Law Studies, Vol. 72/1998, str. 42.
[4] *Ibid*., str. 46.
[5] The General Orders No. 100: Instructions for the Government of the Armies of the United States in the Field (Lieber Code), International Humanitarian Law Database, čl. 16., Dostupno na https://ihl-databases.icrc.org/en/ihl-treaties/liebercode-1863 (26.9.2023)
[6] *Ibid*., čl. 22.
[7] *v. npr*. Petrogradska deklaracija 1868, Deklaracija o zabrani upotrebe metaka koji se u tijelu lako raširi ili spljošte (dum-dum meci) 1899, VIII Haška konvencija 1907.
[8] Andrassy, Juraj; Bakotić, Božidar; Seršić, Maja; Vukas, Budislav, Međunarodno pravo - 3. dio, Školska knjiga, Zagreb, 2006, str. 124-125.

konvencije iz 1899. i 1907. godine, Ženevske konvencije iz 1949. godine i Dopunski protokoli uz njih iz 1977. godine. Navedenim konvencijama uspostavljeno je ono što se danas naziva međunarodnim humanitarnim pravom a čiji je glavni cilj ograničiti učinke oružanog sukoba i humanizirati ih.

Međutim, napredak znanosti i tehnologije, kao i njihovo korištenje u ratne svrhe, nije se zaustavio. Tokom zadnjih 50 godina od donošenja tih dokumenata došlo je do nezapamćenog razvoja u području informatičkih tehnologija. Kako se svijet sve više oslanjao na svakodnevnu upotrebu računala i interneta postalo je jasno da je riječ o najbržoj i najvećoj tehnološkoj revoluciji u povijesti čovječanstva.[9] Broj pojedinaca koji se aktivno koriste internetom porastao je s 16 milijuna u 1995. godini na više od 5,2 milijarde sredinom 2023. godine.[10] Osim pojedinaca i mnoge tvrtke su prihvatile informacijske tehnologije u vođenju poslova. Tvornice i postrojenja počele su koristiti informatičke sustave za proizvodnju proizvoda brže i učinkovitije nego ikad prije. Distribucijske mreže za vodu i energiju koriste se informacijskim tehnologijama, jednako kao i transportni sustavi, zdravstvo i financijski sektori.[11] Istovremeno, vojna uporaba računalnih sustava i mreža, koji se istovremeno koriste u civilne svrhe, eksponencijalno je porasla.[12] Zapovijedanje i organizacija vojnih snaga, logistika pa čak i precizno navođenje oružja može se koordinirati putem sustava i mreža koje omogućuju široku razmjenu informacija.[13] Riječ je o istim sustavima i mrežama koji se svakodnevno koriste i u civilne svrhe. Ta međupovezanost i međuzavisnost između civilne i vojne računalne infrastrukture povećala je rizik da će kibernetičko ratovanje uzrokovati velika stradanja civila i uništenje civilnih objekata.

Iako se još sredinom 1990-ih godina počela razmatrati mogućnost kibernetičkog ratovanja, ta tema je brzo nestala iz javnog diskursa.[14] To se promijenilo 2007. godine kada je, kao dio šireg političkog sukoba između Estonije i Rusije oko izmještanja spomenika iz sovjetskog doba, Estonija pretrpjela masovne kibernetičke napade u trajanju od tri tjedna.[15] Prepoznajući prijetnju koju kibernetički napadi predstavljaju NATO je pokrenuo veliki

[9] Melzer, Nils, "Cyberwarfare and International Law", UNIDR Resources, 2011, str. 3., Dostupno na: https://unidir.org/sites/default/files/publication/pdfs//cyberwarfare-and-international-law-382.pdf (26.9.2023.)
[10] *v. više*. Datreportal, https://datareportal.com/global-digital-overview (26.9.2023)
[11] Lin, Herbert, "Cyber conflict and international humanitarian law", International Review of the Red Cross, Vol 94/2012, str. 516.
[12] Melzer, *op. cit*. (bilj. 9), str. 3.
[13] Lin, *op. cit*. (bilj. 11), str. 516.
[14] Schmitt, Michael, N., "The Law of Cyber Warfare: Quo vadis?", Stanford Law and Policy Review, Vol. 25/2014, str. 269-270.
[15] Schmidt, Andreas, "The Estonian Cyberattacks", 2013, str. 1-2. Dostupno na: https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks (26.9.2023.)

istraživački projekt kako bi se provela analiza međunarodnog prava koje regulira kibernetičko ratovanje što je u konačnici rezultiralo izradom prvog, a zatim i znatno proširenog drugog izdanja *Tallinnskog priručnika o međunarodnom pravu primjenjivom na kibernetičko ratovanje 2.0* (u daljnjem tekstu: Tallinnski priručnik 2.0). Kibernetički napadi na Estoniju nisu bili jedini primjer novog oblika ratovanja. Uporaba kibernetičkih sredstava u ratne svrhe bila je prisutna i u rusko-gruzijskom sukobu 2008. godine kao i u trenutnom ratu u Ukrajini. Možda najpoznatiji primjer kibernetičkog napada predstavlja Stuxnet, sofisticirani računalni crv[16] kojeg su dizajnirale američke i izraelske obavještajne službe za napad na industrijske upravljačke sustave nuklearne elektrane, a koji je osmišljen kako bi se onesposobio iranski nuklearni program.[17]

Sve veća učestalost takvih kibernetičkih napada otvorila je brojna pitanja o primjeni međunarodnog humanitarnog prava koji kao cilj postavlja zaštitu civila i civilnih objekata. Primjena tradicionalnih odredaba, pravila i terminologije međunarodnog humanitarnog prava, pisanih i usvojenih dok kibernetičke operacije još nisu bile ni u svojim začetcima čini se jako teška. Brojne specifičnosti kibernetičkih napada, između ostalog činjenica da se ne provode uporabom kinetičke sile, da se provode u virtualnom prostoru gdje istovremeno djeluje velik broj ljudi te da infrastruktura toga prostora ima i civilnu i vojnu namjenu, onemogućava primjenu pravila i načela međunarodnog humanitarnog prava i otežava zaštitu civila i civilne imovine.

Stoga će svrha ovog rada biti pobliže objasniti probleme i poteškoće koje se pojavljuju kod provođenja kibernetičkih napada i odgovoriti na sljedeća pitanja. Može li se međunarodno humanitarno pravo primijeniti na kibernetičke napade? Te, ako je primjenjivo, kako se pravila i načela tog režima, a posebice pravila razlikovanja, proporcionalnosti i mjera opreza, primjenjuju na kibernetičke napade?

[16] Računalni crvi su samostalni programi koji se sami umnožavaju i šire putem računalne mreže bez interakcije korisnika. Većina se računalnih crva smatra zlonamjernim i nepoželjnim programima. *v. više*: https://www.cert.hr/crvi/ (27.9.2023).
[17] Baenzer, Marie; Robin, Patrice, Stuxnet, 2018, str. 4. Dostupno na: https://www.researchgate.net/publication/323199431_Stuxnet (26.9.2023).

2. KIBERNETIČKI NAPADI - NOVA METODA RATOVANJA

Ratovanje se desetljećima provodilo u četiri domene - na kopnu, moru, u zraku i u svemiru. S razvojem tehnologije, sve bržim umrežavanjem svijeta i porastom kibernetičkih napada, definirana je i peta domena - kibernetički prostor. Kibernetički prostor može se definirati kao virtualni prostor stvoren s pomoću globalno umreženih računala.[18] To je globalno povezana mreža digitalnih informacija i komunikacijskih infrastruktura, uključujući internet, telekomunikacijske mreže te računalne sustave.[19] U kibernetičkom prostoru moguće je provoditi razne aktivnosti u kojima sudjeluju i pojedinci i države.[20] Pa tako osobe mogu dijeliti informacije, međusobno komunicirati, sudjelovati u raspravama i razmjenjivati ideje. To doprinosi gospodarskom razvoju, omogućuje povezivanje i daljnji napredak u informacijskom i komunikacijskom području. No, u kibernetičkom prostoru moguće je provoditi i kibernetičke operacije.

Tallinnski priručnik 2.0 definira kibernetičke operacije kao "*korištenje kibernetičkih sposobnosti za postizanje ciljeva u ili kroz kibernetički prostor*".[21] U takvu definiciju kibernetičkih operacija spadao bi i pojam kibernetičkog napada. Ipak, većina kibernetičkih napada koje spadaju pod pojam kibernetičkih operacija nema nikakve veze s oružanim sukobom i pravilima međunarodnog humanitarnog prava koja se na njega primjenjuju.[22] Primjer toga je kibernetički kriminal koji se općenito definira kao "*korištenje računalnih sredstava za počinjenje nezakonitog djela*".[23] Kao takav, kibernetički kriminal obuhvaća vrlo širok raspon nedopuštenih aktivnosti, kao što su prijevare putem interneta ili upad na računala i krađa podataka, a koje se izvode pomoću kibernetičkih napada. Također, općenito se podrazumijeva da takve kibernetičke napade poduzimaju pojedinci, a ne države.[24] O takvim kibernetičkim napadima, koji se ne izvode u kontekstu oružanog sukoba neće biti riječi u ovom radu.

Opseg ovog rada prvenstveno će biti ograničen na one kibernetičke napade koje se izvode u kontekstu oružanih sukoba. Tallinnski priručnik 2.0 definira takve kibernetičke

[18] *kibernetički prostor*, Hrvatska enciklopedija, mrežno izdanje, Leksikografski zavod Miroslav Krleža, 2021, Dostupno na: https://www.enciklopedija.hr/natuknica.aspx?id=68098 (26.9.2023).
[19] Melzer, *op. cit*. (bilj. 9), str. 4.
[20] *Ibid.*
[21] Schmitt, Michael (ur.), Tallinn Manual 2.0 on the International law Applicable to Cyber Operations, Cambridge University Press, 2017, str. 564. (u daljnjem tekstu: Tallinn Manual 2.0).
[22] International Committee of the Red Cross, International humanitarian law and the challenges of contemporary armed conflicts - Report, 32nd International Conference of the Red Cross and the Red Crescent, 2015, str. 39.
[23] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J., "The Law of Cyber-Attack", California Law Review, Vol.100/2012, str. 22.
[24] *Ibid*. str. 19.

napade kao "*kibernetičku operaciju, ofenzivnu ili obrambenu, za koju se razumno očekuje da će uzrokovati ozljede ili smrt osoba ili štetu ili uništenje objekata*".[25] Kibernetički napadi mogu uzrokovati uništenje financijskih podataka što može dovesti do pada tržišta dionica, ili ometanje elektrodistribucije mreže što će prouzrokovati nestanak struje. Kibernetički napadi također mogu biti i smrtonosni kada na primjer, taj nestanak struje u kontroli zračnog prometa dovede do pada zrakoplova. Sinonim takvim kibernetičkim napadima je pojam kibernetičkog ratovanja koji se definira kao "*operacije protiv računala ili računalnog sustava putem toka podataka, kada se koriste kao sredstva i metode ratovanja u kontekstu oružanog sukoba, kako je definirano prema međunarodnom humanitarnom pravu*".[26] Stoga će se radi lakše preglednosti u nastavku rada pojmovi kibernetička operacija, kibernetički napad i kibernetičko ratovanje koristiti kao sinonimi, a označavat će sva ona sredstva i metode ratovanja koja se koriste u kontekstu oružanog sukoba kako je definiran u međunarodnom humanitarnom pravu.

Kibernetički napadi na Estoniju 2007. godine, rusko-gruzijski sukob 2008. godine, američki rat protiv ISIL-a u Afganistanu i, najrecentnije, rat u Ukrajini pokazuju da je kibernetičko ratovanje već široko rasprostranjeno.[27] Trenutno je više od 100 zemalja, uključujući Republiku Hrvatsku razvilo ili se sprema razviti svoje vlastite snage za kibernetičko ratovanje.[28] Kibernetičko ratovanje može uzrokovati uništenje civilnih objekata i velika stradanja civilne populacije koja se u najvećoj mjeri koristi kibernetičkim prostorom. Tradicionalna pravila za vođenje neprijateljstava, utemeljena na međunarodnom humanitarnom pravu, određivala su kako civilnu populaciju zaštititi. No zbog specifičnosti kibernetičkog prostora i kibernetičkih napada koji se u njemu provode, postavlja se pitanje mogu li se ta tradicionalna pravila međunarodnog humanitarnog prava primijeniti i na kibernetičke napade?

[25] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Rule 92, str. 415.
[26] International humanitarian law and the challenges of contemporary armed conflicts - Report, *op. cit.* (bilj. 22), str 39.
[27] Pascucci, Peter, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", Minnesota Journal of International Law, 215/2017, str. 425.
[28] Ranger, Steve, Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar, Techrepublic, 2014, Dostupno na: http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/ (26.9.2023).

3. PRIMJENJUJE LI SE MEĐUNARODNO HUMANITARNO PRAVO NA KIBERNETIČKE NAPADE?

Dok *jus ad bellum* utvrđuje zabranu upotrebe sile, *jus in bello* odnosno međunarodno humanitarno pravo nameće ograničenja o tome kako se neprijateljstva mogu voditi nakon što oružani sukob izbije**.** Odnosno, jednom kada je država ušla u sukob pravila korištenja sile regulirana su međunarodnim humanitarnim pravom. To pravo pretpostavlja određena ograničenja ratovanja koja država mora poštivati. Utemeljeno je pretežito na Haškim i Ženevskim konvencijama i Dopunskim protokolima uz njih kao i na običajnom pravu.

Preambula Dopunskog protokola Ženevskim konvencijama od 12. kolovoza 1949. o zaštiti žrtava međunarodnih oružanih sukoba (u daljnjem tekstu: Protokol I.) iz 1977. godine navodi da je cilj međunarodnog humanitarnog prava "*zaštita žrtava oružanog sukoba*".[29] Iako je Protokol I. danas široko prihvaćen, određene države poput SAD-a Izraela i Turske, ali i Irana, Indije i Pakistana nisu njegove stranke. Na njih će se primjenjivati samo one odredbe Protokola I. koje su postale dijelom međunarodnog običajnog prava.

Ukoliko dođe do izbijanja oružanog sukoba, međunarodno humanitarno pravo definira zaštitu za one koji ne sudjeluju u neprijateljstvima i ograničava izbor zaraćenih stranaka u sredstvima i metodama ratovanja. Odredbe međunarodnog humanitarnog prava ne spominju izričito kibernetičke napade. Međutim, odsutnost specifičnih odredbi za kibernetičke napade ne znači da takve operacije ne podliježu pravilima međunarodnog humanitarnog prava. Od svojih početaka, međunarodno humanitarno pravo pretpostavlja tehnološke promjene i razvitak novih načina ratovanja i proširuje svoje odredbe i na takve slučajeve. Na primjer, Martensova klauzula koja se nalazi u preambuli IV. Haške konvencije iz 1907. godine navodi da čak i u slučajevima koji nisu uređeni ugovornim pravom "*stanovništvo i ratnici ostaju pod zaštitom i vladavinom načela međunarodnog prava koja proizlaze iz običaja ustanovljenih među civiliziranim narodima, iz zakona čovječnosti i zahtjeva javne savjesti*".[30] Martensova klauzula ponovno je izražena u suvremenim konvencijama kao i presudama međunarodnih sudova, te je ujedno postala i dio običajnog međunarodnog prava.[31] Ona služi kao osiguranje da praznine u postojećem pravnom režimu ne dovedu do nedostatka zaštite pojedinaca u oružanim sukobima

[29] Preambula, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, (u daljnjem tekstu Protokol I), 1977, International Humanitarian Law Database, Dostupno na https://ihldatabases.icrc.org/en/ihl-treaties/api-1977 (26.9.2023).
[30] Preambula, Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 1907, International Humanitarian Law Database, Dostupno na https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907 (26.9.2023).
[31] Andrassy, Bakotić, Seršić, Vukas, *op. cit.* (bilj. 8), str. 131.

te naglašava važnost međunarodnog običajnog prava u zaštiti pojedinaca. Nadalje, članak 36. Protokola I. navodi da "*Prilikom proučavanja, usavršavanja, nabavljanja ili prihvaćanja novog oružja, novih sredstava ili nove metode ratovanja visoka je stranka ugovornica obvezana utvrditi bi li njihova upotreba, u nekim ili u svim okolnostima, bila zabranjena ovim Protokolom ili bilo kojim drugim pravilom međunarodnog prava*".[32] Možda i najbitnije, u savjetodavnom mišljenju o dopuštenosti prijetnje ili uporabe nuklearnog oružja, Međunarodni sud smatrao je da se utvrđena načela i pravila međunarodnog humanitarnog prava primjenjiva u oružanim sukobima primjenjuju "*na sve oblike ratovanja i na sve vrste oružja*", uključujući i "*ona iz budućnosti*".[33] Navedeni primjeri pokazuju da su pravila međunarodnog humanitarnog prava dovoljna široka kako bi se mogla primijeniti na nove tehnologije, uključujući i kibernetičke operacije.

Ipak, među državama se razvila velika rasprava o tome može li se međunarodno humanitarno pravo primjenjivati u kibernetičkom prostoru. Na trećem sastanku UN-ove Skupine vladinih stručnjaka o razvoju na području informacija i telekomunikacija u kontekstu međunarodne sigurnosti (u daljnjem tekstu: Skupina) održanom od 2012. do 2013. godine, iako je istaknuto da se međunarodno pravo primjenjuje na kibernetički prostor, nije navedeno odnosi li se to i na međunarodno humanitarno pravo.[34] Na četvrtom sastanku Skupine održanom od 2014. do 2015. godine, na kojem se raspravljalo o tome kako se međunarodno pravo primjenjuje na djelovanje država u kibernetičkom prostoru, nekoliko država se nije slagalo s primjenjivošću međunarodnog humanitarnog prava i temeljnih pravila tog pravnog režima na kibernetički prostor.[35] Ni na petom sastanku Skupine održanom od 2016. do 2017. godine, zbog protivljenja Kube, Rusije i Kine nije postignut konačni konsenzus o tom pitanju.[36] S druge strane, postoji veliki broj država koje se slažu s primjenom međunarodnog humanitarnog prava u kibernetičkom prostoru, a među njima su Argentina, Australija, Brazil, Kanada, Čile,

[32] Protokol I, *op. cit.* (bilj. 29), čl. 36.
[33] ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory opinion, 1996, paragraf 86, Dostupno na: https://www.icj-cij.org/sites/default/files/case-related/95/095-19960708-ADV-01-00-EN.pdf (26.9.2023).
[34] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 68th Session, UN Document A/68/98, 2013, p. 19.
[35] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 70th Session, UN Document A/70/174, p. 28.
[36] Schmitt, Michael; Vihul, Liis, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms" Just Security, 2017, Dostupno na: https://www.justsecurity.org/42768/international-cyber-law- (26.9.2023).

Kolumbija, Egipat, Pakistan, Švicarska, Ujedinjeno Kraljevstvo, SAD, Urugvaj, Zimbabve kao i države članice EU.[37]

Međunarodni odbor Crvenog križa[38] (u daljnjem tekstu: MOCK) zauzeo je stav da se međunarodno humanitarno pravo može primijeniti na kibernetički prostor i da uporaba kibernetičkih sposobnosti u oružanom sukobu mora biti u skladu sa svim načelima i pravilima međunarodnog humanitarnog prava.[39] Sličnog je stajališta i Tallinnski priručnik 2.0 koji navodi da "*kibernetičke operacije koje se izvode u kontekstu oružanog sukoba podliježu pravu oružanog sukoba*".[40] Prema tome, može se zaključiti kako se međunarodno humanitarno pravo može primijeniti na kibernetičke napade. Naravno, mora biti riječ o onim kibernetičkim napadima koji se provode u kontekstu oružanog sukoba, jer su, jednako kao i kod tradicionalnih kinetičkih napada, samo tada pravila međunarodnog humanitarnog prava primjenjiva.[41]

4. MOGU LI SE KIBERNETIČKE OPERACIJE SMATRATI NAPADOM U KONTEKSTU MEĐUNARODNOG HUMANITARNOG PRAVA?

Jedno od pitanja o kojima se najviše raspravljalo u vezi s kibernetičkim operacijama tijekom oružanih sukoba jest ono o značenju napada.[42] U međunarodnom humanitarnom pravu pojam napada ima posebno značenje.[43] Pravila, zabrane, ograničenja i zahtjevi međunarodnog humanitarnog prava primjenjuju se samo na one kibernetičke operacije koje se smatraju napadom.[44] Pa tako na primjer, ukoliko se kibernetička operacija ne smatra napadom,

[37] Second 'Pre-Draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security, 2020, Dostupno na https://ict4peace.org/wp-content/uploads/2020/12/200527-oewg-ict-revised-pre-draft.pdf (26.9.2023).

[38] MOCK je neovisna i neutralna organizacija, koja se izričito spominje u Dopunskim protokolima, a kao zadatak ima pružanje pomoći žrtvama rata i oružanog sukoba, te osiguranje primjene i poštovanja međunarodnog humanitarnog prava. Također, MOCK ima značajnu ulogu i u razvitku međunarodnog humanitarnog prava.

[39] International humanitarian law and the challenges of contemporary armed conflicts - Report, *op. cit.* (bilj. 22), str 18.

[40] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Rule 80, str. 375.

[41] Pa se tako međunarodno humanitarno pravo nije primjenjivalo u slučaju kibernetičkih napada na Estoniju 2007. godine jer se takva situacija nije smatrala oružanim sukobom. Nasuprot tome, međunarodno humanitarno pravo primjenjivalo se na kibernetičke napade koji su se dogodili tijekom oružanog sukoba između Rusije i Gruzije 2008. godine.

[42] Schmitt, *op. cit.* (bilj. 14), str. 293.

[43] Pascuci, *op. cit.* (bilj. 27), str 442.

[44] Ipak, primjena određenih pravila međunarodnog humanitarnog prava ne ovisi o tome je li došlo do napada. Nekoliko pravila, poput članka 48. Protokola I, primjenjuje se na sve „vojne operacije", dok se posebna zaštita koja se pruža određenim kategorijama osoba i objekata, poput objekata iz članka 54. ili osoba iz članka 12. Protokola I, pruža i u slučaju da do napada nije došlo. *v. više*. Dormann, Kunt; Gisel, Laurent; Rodenhauser, Tilman, "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts", International Review of the Red Cross, Vol. 102/2020, str. 322-329.

zapovjednici nisu obvezni primjenjivati pravilo proporcionalnosti.[45] Zato je prvo potrebno definirati koje se kibernetičke operacije mogu smatrati napadom u kontekstu međunarodnog humanitarnog prava.

Protokol I. definira napad kao "*čine nasilja protiv protivnika, bilo da su ti čini napadački ili obrambeni*".[46] Navedena definicija nastala je u doba kada su se napadi izvodili gotovo isključivo kinetičkim sredstvima. Kinetička sredstva, poput bombardiranja ili granatiranja, su sama po sebi nasilna. Posljedično, korištenje ne nasilnih sredstava, nije se smatralo napadom. Ipak, pojavom novih sredstava ratovanja, kao što su kemijski i biološki napadi, pojam nasilja nije više bio ograničen samo na kriterij sredstva. Korištenje kemijskih i bioloških oružja, koja samo po sebi nisu nasilna sredstva, svejedno se smatra napadom.[47] To je dovelo do toga da danas postoji široko slaganje da se pojam nasilja ne bi trebao restriktivno tumačiti tako da se odnosi samo na sredstva napada.[48] Shodno tome, prihvaćeno je stajalište da se pojam nasilja može odnositi ili na sredstva ratovanja ili na njihove učinke, što znači da operacija koja uzrokuje nasilne učinke može biti napad čak i ako sredstva korištena za izazivanje tih učinaka nisu sama po sebi nasilna.[49]

Slična dilema se pojavljuje i kod kibernetičkih operacija. Jedna od posebnosti kibernetičkih operacija je ta što takvi napadi ne uključuju uporabu kinetičke sile. Ipak, iako kibernetički napad nije kinetičke prirode još uvijek može dovesti do velikih fizičkih razaranja, šteta pa čak i smrti, odnosno može imati nasilne učinke. Pa bi tako slanje računalnog virusa, iako samo po sebi ne predstavlja uporabu kinetičke sile, zbog činjenice da ima nasilne učinke, ipak u kontekstu međunarodnog humanitarnog prava predstavljalo napad i kao takvo bilo podložno primjeni svih pravila tog pravnog režima. No, bitno je za napomenuti da se ne mogu sve kibernetičke operacije smatrati napadima. Određene kibernetičke operacije mogu biti vojno korisne bez da dovedu do nasilnih ili štetnih učinaka.[50] One kibernetičke operacije koje su ekvivalentne špijunaži, širenju propagande, ometanju civilnih komunikacijskih sustava ili drugim sredstvima psihološkog ili ekonomskog ratovanja, zbog nedostatka nasilnih učinaka,

[45] Jensen, Eric, T., „Cyber Attacks: Proportionality and Precautions in Attack", International Law Studies, Vol. 98/2013, str. 201.
[46] Protokol I., *op. cit.* (bilj. 29), čl.49, t.1.
[47] ICTY, The Prosecutor vs. Dusko Tadic, Decision on the defence motion for interlocutary appeal, 1995, paragraf 120-124.
[48] *v. više*. Sohail, Humna, "Fault Lines In The Application Of International Humanitarian Law Cyberwarfare", Journal of Digital Forensics, Security and Law, Vol.17/2022, str. 5; Dinstein, Yoram, "The Conduct of Hostilities under the Law of International Armed Conflict", Cambridge University, 2004, str. 84.
[49] Droege, Cordula, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", International Review of the Red Cross, Vol. 94/2012, str. 557.
[50] Schmitt, *op. cit.* (bilj. 14), str. 293-295.

neće se smatrati napadom u kontekstu međunarodnog humanitarnog prava.[51] Uzimajući u obzir ranije navedeno, Tallinnski priručnik 2.0 navodi da kibernetički napad uključuje svaku „*kibernetičku operaciju, napadačku ili obrambenu, za koju se razumno očekuje da će prouzročiti ozljedu ili smrt osoba ili oštećenje ili uništenje predmeta*".[52] Prihvaćeno je kako od međunarodne skupine stručnjaka koja je sastavljala Tallinnski priručnik 2.0 pa tako i od MOCK-a da barem one kibernetičke operacije koje uzrokuju smrt, ozljede ili fizičku štetu predstavljaju napade prema međunarodnom humanitarnom pravu.[53]

Unatoč slaganju da kibernetičke operacije mogu predstavljati napad, postoje različita stajališta o tome je li kibernetička operacija koja onesposobljava objekt bez njegovog fizičkog oštećenja ili uništenja jednaka napadu prema međunarodnom humanitarnom pravu.[54] Na primjer, ako je, kao posljedica kibernetičkih operacija došlo do pada elektrodistribucijske mreže, to može dovesti do prestanka opskrbe strujom vitalnih usluga kao što su bolnice. Ipak, samo po sebi to ne predstavlja fizičko oštećenje ili uništenje objekta niti dovodi do smrti ili ozljede osoba kao što bi to učinile kinetičke operacije. Takve kibernetičke operacije remete samo funkcioniranje objekata bez nanošenja fizičkog oštećenja. Zato se postavlja pitanje, mogu li se takve kibernetičke operacije smatrati napadima u kontekstu međunarodnog humanitarnog prava?

Kod definiranja koje sve kibernetičke operacije potpadaju pod pojam napada treba biti oprezan. Ukoliko se prihvati uže tumačenje pojma napad onesposobljavanje sustava protuzračne obrane države ili druge kritične vojne infrastrukture a koje izravno ne uzrokuje smrt, oštećenje ili uništenje ne bi se smatralo napadom.[55] U tom slučaju ciljevi međunarodnog humanitarnog prava, a posebice zaštita civila i civilnih objekata ne bi bili ispunjeni. S druge strane, preširoko tumačenje pojma napad značilo bi da bi se sve smetnje u računalnim sustavima, uključujući i one minorne poput prekida komunikacije putem e-pošte, smatrale napadima zbog čega bi se izašlo iz okvira međunarodnog humanitarnog prava.[56]

Ipak, uzmimo za primjer elektrodistribucijsku mrežu koja je stavljena izvan funkcije zbog fizičkog oštećenja nasuprot one koja više ne funkcionira zbog smetnji u računalnom sustavu koji ju kontrolira. Bilo bi neshvatljivo da se od ta dva slučaja, oba koja rezultiraju prekidom opskrbe električnom energijom, jedan tumači kao napada a drugi ne. Sličnog je

[51] Droege, op. cit. (bilj. 49), str. 559-560.
[52] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Rule 92, str. 415.
[53] International humanitarian law and the challenges of contemporary armed conflicts - Report, *op. cit.* (bilj. 22), str. 41-42.
[54] Schmitt, *op. cit.* (bilj. 14), str. 293-295.
[55] Melzer, *op. cit.* (bilj. 9), str. 26.
[56] Droege, *op. cit.* (bilj. 49), str. 559.

stajališta i MOCK koji je zauzeo stav da kibernetička operacija osmišljena da onesposobi računalo ili računalnu mrežu tijekom oružanog sukoba predstavlja napad kako je definiran u međunarodnom humanitarnom pravu bez obzira je li objekt onesposobljen uništenjem ili na bilo koji drugi način.[57] MOCK takvo tumačenje temelji na činjenici da se definicija vojnih ciljeva iz članka 52. Protokola I. odnosi i na neutralizaciju, a ne samo na uništenje ili zarobljavanje kao moguće rezultate napada.[58] Također, MOCK smatra da bi pretjerano restriktivno shvaćanje pojma napada bilo teško uskladiti s ciljem i svrhom pravila o vođenju neprijateljstava, a posebice onim pravilima kojima se osigurava zaštita civilnog stanovništva i civilnih objekata.[59] Sličnog je stajališta i Tallinnski priručnik 2.0. Većina međunarodne skupine stručnjaka se složila da se "*ometanje funkcionalnosti kvalificira kao šteta ako ponovno uspostavljanje funkcionalnosti zahtijeva zamjenu fizičkih komponenti*".[60] Manji dio stručnjaka dodatno je smatrao da će kibernetička operacija predstavljati napad čak i ako ponovno uspostavljanje funkcionalnosti zahtijeva samo ponovnu instalaciju operativnog sustava ili određenih podataka.

Uzimajući u obzir sve ranije navedeno može se zaključiti da kibernetička operacija predstavlja napad u smislu međunarodnog humanitarnog prava kada uzrokuje smrt ili ozljedu, fizičko uništenje ili štetu, ali i onda kada uzrokuje gubitak funkcionalnosti objekta. Na takve će se kibernetičke operacije moći primijeniti pravila međunarodnog humanitarnog prava.

5. PRIMJENA GLAVNIH PRAVILA MEĐUNARODNOG HUMANITARNOG PRAVA NA KIBERNETIČKE NAPADE

Kako bi se mogao postići glavni cilj međunarodnog humanitarnog prava, uspostavljana su određena pravila vođenja neprijateljstava. Postoje tri glavna pravila koja reguliraju način na koji stranka u oružanom sukobu može izvoditi vojne operacije, odnosno provoditi neprijateljstva, a koja su ujedno postala i dio običajnog prava - pravilo razlikovanja, proporcionalnosti i poduzimanja mjera opreza.[61] Kao što je ranije prikazano, pravila međunarodnog humanitarnog prava su dovoljno široka da se primjenjuju na kibernetičke operacije, i to one kibernetičke operacije koje se mogu smatrati napadom. No, zbog specifičnosti kibernetičkog prostora i kibernetičkih napada i njihove razlike u odnosu na

[57] Dormann; Laurent, *op. cit.* (bilj. 44), str. 313.
[58] *Ibid.*
[59] *Ibid.* str. 314.
[60] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 92, str. 416.
[61] MOCK, Međunarodno humanitarno pravo – odgovori na vaša pitanja, 2012, str. 46., Dostupno na: https://www.hck.hr/UserDocsImages/publikacije/0703_002_IHL-answers_Couv_LR.pdf (26.9.2023).

tradicionalna sredstva ratovanja, postoje određene teškoće u primjeni tih pravila. Zbog toga je potrebno pobliže objasniti kako se pravila međunarodnog humanitarnog prava primjenjuju na takve kibernetičke napade, o čemu će više riječi biti u nastavku poglavlja.

5.1. PRAVILO RAZLIKOVANJA

Osnovno pravilo i jedno od temeljnih načela međunarodnog humanitarnog prava je pravilo razlikovanja. Protokol I. navodi da "*stranke sukoba moraju u svako doba razlikovati civilno stanovništvo od boraca, kao i civilne objekte od vojnih ciljeva, te prema tome usmjeriti svoje vojne operacije samo na vojne ciljeve*".[62] Pravilo razlikovanja nalazi se i u ostalim odredbama Protokola I., od kojih mnoge odražavaju međunarodno običajno pravo. Pa tako, članak 51. zabranjuje napade na civilno stanovništvo ili pojedine civile, članak 52. zabranjuje napade na civilne objekte dok članak 54. zabranjuje napade na objekte neophodne za opstanak civilnog stanovništva.[63] Važnost načela razlikovanja istaknuo je i Međunarodni sud kada je zaključio da "*države nikada ne smiju učiniti civile predmetom napada i stoga nikada ne smiju koristiti oružje koje nije u stanju razlikovati civilne od vojnih ciljeva*".[64]

Osnovni zadatak načela razlikovanja je ograničiti napade samo na osobe koje sudjeluju u borbi te samo na objekte koji se mogu smatrati vojnim ciljevima. Namjerno gađanje civilnih objekata, osim što je kršenje međunarodnog humanitarnog prava, predstavlja i ratni zločin.[65] U kontekstu kibernetičkih operacija načelo razlikovanja zahtijevalo bi od osobe koja poduzima kibernetički napad da uloži razumne napore kako bi napravila razliku između boraca i civila te civilnih i vojnih objekata te da se suzdrži od namjernih napada na civile i civilne objekte. U određenim slučajevima ta razlika je vrlo jasna. Na primjer, ukoliko je kibernetički napad usmjeren protiv radarskih sustava namijenjenih vojnoj uporabi takav napad bio bi u skladu s načelom razlikovanja. S druge strane, kad bi kibernetički napad bio usmjeren na bolnice, takav napad ne bi bio u skladu s načelom razlikovanja. No, poteškoće se javljaju kada razlika između vojnih i civilnih objekata nije potpuno jasna. Određeni objekti mogu istovremeno biti korisni kako civilnom stanovništvu tako i vojsci. Iako postoji presumpcija da se, u slučaju sumnje radi li se o civilnom ili vojnom objektu, objekt koji je redovno namijenjen civilnoj uporabi ne smatra vojnim ciljem mogu se pojaviti poteškoće kod određivanju prema kojim je točno objektima dopušteno izvršiti kibernetički napad. Osim toga, uključenost civila u provođenje aktivnosti

[62] Protokol I., *op. cit.* (bilj. 28), čl. 48.
[63] *Ibid.* čl. 51., čl. 52., čl. 54.
[64] ICJ, *op. cit*. (bilj. 33), paragraf 75.
[65] Rimski statut Međunarodnog kaznenog suda, Narodne novine, Međunarodni ugovori, 5/2001, čl. 8(2)(b)(ii).

unutar kibernetičkog prostora otvara pitanja o tome koje osobe mogu biti meta kibernetičkih napada te tko može izvesti kibernetičke napade? O tim poteškoćama u primjeni pravila razlikovanja bit će riječ u nastavku poglavlja.

5.1.1. Objekti

Pravila vođenja oružanog sukoba, a osobito načelo razlikovanja, temelje se na osnovnoj ideji da je potrebno razlikovati civilne i vojne objekte.[66] Ukoliko objekt služi u vojne svrhe napad je dopušten, dok ukoliko služi u civilne tada uživa zaštitu i napad nije dopušten. Nadalje, općeprihvaćeno je pravilo međunarodnog humanitarnog prava da jednom kada objekt po svojoj prirodi, po svojem smještaju, po svojoj namjeni ili po svojoj upotrebi djelotvorno pridonosi vojnoj akciji i čije potpuno ili djelomično uništenje, zauzimanje ili neutralizacija donosi u danim okolnostima očitu vojnu prednost tada takav objekt postaje vojni cilj.[67] Pa bi tako škole, bolnice ili crkve, koje su u početku smatrane civilnim objektom, izgubile svoju zaštitu i postale legitimnim vojnim ciljem ako se u njima nalaze neprijateljski vojnici ili se koriste kao skladište naoružanja te tako djelotvorno pridonose vojnoj akciji.[68] Sam opseg korištenja je nebitan, pa se danas smatra da objekt postaje vojni cilj čak i ako je njegova vojna uporaba samo marginalna u usporedbi s njegovom civilnom upotrebom. Na primjer, ukoliko određena elektrana daje samo mali postotak energije korištene u vojnim operacijama, ona se i dalje može smatrati vojnim ciljem.[69]

5.1.1.1. Objekti dvojne namjene

Glavna poteškoća u primjeni pravila razlikovanja na kibernetičke napade leži u činjenici da je većina kibernetičke infrastrukture zapravo objekt dvojne namjene (*eng. dual-use object*). Objekti dvojne namjene su oni koji se istovremeno mogu koristiti u civilne i u vojne svrhe. Za razliku od konvencionalnih fizičkih vojnih instalacija, koje je relativno lako razlikovati i odvojiti od civilne infrastrukture, civilna i vojna kibernetička infrastruktura obično je međusobno povezana.[70] Danas se čak devedeset pet posto vojnih komunikacija u nekoj fazi prijenosa koristi podvodnim optičkim kabelima, ruterima i serverima koji se također koriste u

[66] Droege, *op. cit.* (bilj. 49), str. 541.
[67] MOCK, Customory IHL - Rules, Rule 10, Dostupno na: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule10#Fn_A84730F9_00002 (26.9.2023); Protokol I., *op. cit.* (bilj. 28), čl. 52, st. 2.
[68] Andrassy, Bakotić, Seršić, Vukas, *op. cit.* (bilj. 8), str. 149.
[69] Droege, *op. cit.* (bilj. 49), str. 563.
[70] Fenton, Hensey, A., III, "Proportionality and its applicability in the realm of cyber-attacks", Duke Journal of Comperative & International Law, Vol. 29/2019, str. 349.

civilne svrhe.[71] Isto tako, civilna vozila, brodovi i zrakoplovi opremljeni su navigacijskom opremom koja se oslanja na GPS.[72] No, osim što se GPS svakodnevno koristi u civilne svrhe, ugrađen je i u vojna vozila a može se koristiti i za ciljanje te uporabu oružja. Također, internet, a posebice društvene mreže, koriste se tijekom oružanih sukoba za prijenos važnih vojnih informacija.[73] Izuzev malobrojnih zatvorenih mreža koje su specifično namijenjene za vojnu uporabu, navedeni primjeri pokazuju da je vrlo teško razlikovati isključivo civilnu od isključivo vojne infrastrukture. Upravo ta povezanost između civilne i vojne kibernetičke infrastrukture otežava pravilnu primjenu pravila razlikovanja i predstavlja veliku opasnost za civilnu populaciju i civilne objekte.

Kao što je već ranije navedeno pravilo razlikovanja zahtjeva da napadi moraju biti ograničeni na one objekte koji se mogu smatrati vojnim ciljem. Protokol I. definira vojne ciljeve kao "*one objekte koji po svojoj prirodi, po svom smještaju, po svojoj namjeni ili po svojo upotrebi djelotvorno pridonose vojnoj akciji i čije potpuno ili djelomično uništenje, zauzimanje ili neutralizacija donosi u danim okolnostima očitu vojnu prednost*".[74] Ukoliko objekt ne ispunjava te elemente ne može se smatrati legitimnim vojnim ciljem. U slučaju sumnje koristi li se objekt koji je inače namijenjen u civilne svrhe za doprinos vojnoj akciji, mora se pretpostaviti da i dalje uživa zaštitu kao civilni objekt.[75]

Baveći se problematikom objekata dvojne namjene Tallinnski priručnik 2.0 navodi da su svi objekti dvojne namjene vojni ciljevi.[76] Sličnog je stajališta i MOCK koji ističe da kada se određeni objekt istovremeno koristi u civilne i u vojne svrhe taj objekt tada postaje vojni cilj i može biti predmetom napada kibernetičkim sredstvom.[77] Takvo tumačenje, iako na prvi pogled pojednostavljuje proces razlikovanja civilnih i vojnih objekata u kibernetičkom prostoru, potencijalno otvara nove probleme. Kada se takvo tumačenje primjeni na kibernetičke operacije dolazi se do zaključka da bi gotovo svi dijelovi međunarodne kibernetičke infrastrukture, upravo zbog činjenice njene međupovezanosti i međuzavisnosti, mogli biti podložni kibernetičkim napadima. To otvara mogućnost da se optički kabeli, serveri i sateliti,

[71] Antolin- Jenkins, Vida, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?", Naval Law Review. Vol.132/2008, str. 140.
[72] GPS, odnosno Global Positioning System, je satelitski radionavigacijski sustav za određivanje položaja na Zemlji. Čini ga skupina satelita koji stalno kruže oko Zemlje i koji odašilju radio signale što omogućuje GPS-prijamniku da odredi svoj položaj.
[73] Schmitt, *op. cit.* (bilj. 14), str. 298.
[74] Protokol I., *op. cit.* (bilj. 28), čl. 52.
[75] *Ibid.*
[76] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Rule 101, str. 445.
[77] International humanitarian law and the challenges of contemporary armed conflicts - Report, *op. cit.* (bilj. 22), str. 42.

o kojima ovise civilni sustavi i koji osim civilnih prenose i vojne informacije, smatraju vojnim ciljevima. Zbog velike količine objekata u kibernetičkom prostoru koji bi se stoga smatrali vojnim ciljevima, pravilo razlikovanja izgubilo bi svoju svrhu.[78] Kako bi pravilo razlikovanja ispunilo svoju svrhu te kako bi se zaštitili civili i civilni objekti, opravdanost kibernetičkih napada na objekte dvojne namjene mora se procjenjivati od slučaja do slučaja uz stalnu primjenu ograničenja koja uspostavljaju pravila proporcionalnosti i poduzimanje mjere opreza. O pojedinim slučajevima primjene pravila razlikovanja na određene objekte i poteškoćama koje se pojavljuju bit će riječ u nastavku.

5.1.1.1.1. Tvornice i postrojenja

Danas postoji veliki broj kompanija koje proizvode računala, kibernetičke sustave i ostale generičke informatičke alate koji nisu posebno namijenjeni vojsci, ali ih vojne snage često koriste.[79] Ministarstvo obrane SAD-a navodi Microsoft, Verizon i IBM, kompanije koje proizvode civilne sustave i komponente, kao jedne od svojih najvećih dobavljača.[80] S obzirom da se, u tom slučaju, identični hardver odnosno softver koristi i za civilne i za vojne svrhe, moglo bi se zaključiti da bi se sve takve kompanije, odnosno njihove tvornice i postrojenja, mogle smatrati vojnim ciljevima, naravno uz ograničenja uspostavljena pravilima proporcionalnosti i mjerama opreza.[81] Također, ne postoji obaveza da se računala, kibernetički sustavi i ostali generički informatički alati stvarno počnu koristiti prije nego što postanu legitimni vojni ciljevi.[82] Stoga, ako država ima razloge vjerovati da se njezin protivnik sprema nabaviti određeni računalni hardver ili softver koji će upotrjebljavati u vojne svrhe, postrojenja i tvornice koje ih proizvode već bi tada mogli postati vojni ciljevi.[83]

Ipak, kako bi se tvornice i postrojenja mogli kvalificirati kao vojni cilj trebaju ispunjavati dva elementa iz članka 52. Protokola I. – trebaju djelotvorno pridonositi vojnoj akciji i napad na takve objekte treba donijeti očitu vojnu prednost. Prvi element je ispunjen ako objekt po svojoj prirodi, smještaju, namjeni ili uporabi djelotvorno pridonosi vojnoj akciji. Postoji razlika između kibernetičkog oružja, koje po svojoj prirodi ima takav učinak, i

[78] Diamond, Eitan, "Applying International Humanitarian Law to Cyber Warfare", Institute fo National Security Studies, 2014, str. 77-78.
[79] Pascuci, *op. cit.* (bilj. 27), str 437.
[80] *v. više*. U.S. Department of Defense – Contracts, Dostupno na: https://www.defense.gov/News/Contracts/ (26.9.2023).
[81] Schmitt, Michael, N., "Cyber operations and the jus in bello: key issues", International Law Studies, Vol. 87/2011, str. 8.
[82] Geiss, Robin; Lahmann, Henning, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space" Israel Law Review, Vol. 45/2012 str. 385.
[83] Pascuci, *op. cit.* (bilj. 27), str 437.

generičkih informatičkih alata, koji takav učinak nemaju.[84] Stoga se mora napraviti i razlika između tvornica koje razvijaju kibernetičko oružje koji će se koristiti za određeni napad (poput tvornica gdje se razvijao Stuxnet) od onih koji samo opskrbljuju vojsku generičkim informatičkim alatima.[85] U navedenom primjeru, prva tvornica bi predstavlja vojni cilj, dok bi napad na drugu bio zabranjen. Drugi element zahtjeva da napad na takvu tvornicu donosi očitu vojnu prednost. Tallinnski priručnik 2.0 navodi da *"pitanje kvalificira li se tvornica kao vojni cilj ovisi o razmjeru, opsegu i važnosti vojne prednosti"*.[86] No unatoč tome, međunarodna skupina stručnjaka nije uspjela odrediti točan prag za utvrđivanje očite vojne prednosti i prosuđivanje mogu li se takve tvornice smatrati vojnim ciljem.[87] Tu je također najbolje primijeniti ustaljenu praksu da se vojna prednost procjenjuje uzimajući u obzir okolnosti slučaja, uz napomenu da takva prednost mora biti očita, a ne samo hipotetska.

5.1.1.1.2. Društvene mreže

Google Maps koriste anonimne informacije o lokaciji prikupljene s pametnih telefona kako bi korisniku u stvarnom vremenu prikazale lokacije na cestama gdje su prometni zastoji. U veljači 2022. godine, tek nekoliko sati prije početka ruske invazije na Ukrajinu, te su svima dostupne informacije prikazale velike zastoje i kolone na cestama prema rusko-ukrajinskim granicama. To je ubrzo objavljeno na Twitteru, pa su svi korisnici te društvene mreže mogli u realnom vremenu pratiti kretanje ruskih trupa prema granici s Ukrajinom.[88] Iako je Google nekoliko dana kasnije tu uslugu isključio na području Ukrajine,[89] ipak bi dijeljenje takvih informacija, inače javno dostupnih svima s pametnim uređajima i pristupom društvenim mrežama, svaka zaraćena stranka htjela vrlo rado spriječiti. S obzirom na narav takvih usluga i društvenih mreža jedino moguće rješenje bio bi kibernetički napad. No, postavlja se pitanje predstavljaju li društvene mreže legitiman vojni cilj?

S obzirom da društvene mreže mogu služiti i u civilne i u vojne svrhe one su objekt dvojne namjene. Kao što je ranije rečeno, ako se društvene mreže, uz primjenu pravila razlikovanja, proglase vojnim ciljevima, kibernetički napad na njih bi bio dopušten.[90] Ipak, postoje određena ograničenja. Prvenstveno, kako navodi Tallinnski priručnik 2.0, ukoliko se

[84] Droege, *op. cit.* (bilj. 49), str. 567.
[85] *Ibid.*
[86] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 100, str. 438.
[87] *Ibid.*
[88] Cieslak, Mark; Gerken, Tom, Ukraine crisis: Google Maps live traffic data turned off in country, BBC News, 2022, Dostupno na: https://www.bbc.com/news/technology-60561089 (26.9.2023).
[89] Culliford, Elizabeth, Google temporarily disables Google Maps live traffic data in Ukraine, Reuters, 2022, Dostupno na: https://www.reuters.com/technology/google-temporarily-disables-google-maps-live-traffic-data-ukraine-2022-02-28/ (26.9.2023).
[90] Pascuci, *op. cit.* (bilj. 27), str 438.

kibernetička operacija ne smatra napadom, tada društvene mreže niti ne mogu biti kvalificirane kao vojni cilj.[91] Nadalje, i ovdje postoji obveza poštivanja pravila proporcionalnosti i poduzimanja odgovarajućih mjera opreza. Konačno, klasifikacija društvenih mreža poput Twittera, koji sadrži goleme količine informacija od kojih se većina ne koristi u vojne svrhe, kao vojnog cilja stvarala bi brojne probleme. Prihvaćajući takvo stajalište, Tallinnski priručnik 2.0 navodi da društvene mreže ne mogu u cijelosti biti meta kibernetičkog napada već samo njihovi točno određeni dijelovi koji se koriste u vojne svrhe mogu biti smatrani vojnim ciljem.[92]

5.1.1.1.3. Internet

Zbog međusobne povezanosti civilne i vojne internetske infrastrukture, te činjenice da se takva infrastruktura vrlo lako može koristiti u vojne svrhe, otvara se mogućnost da se napadne i internet. Ipak, činjenica da dijelovi internetske infrastrukture mogu biti korišteni u vojne svrhe ne daju pravo napadaču da izvrši napad na internet u cijelosti. MOCK navodi da se analiza o tome kada civilni objekt postaje vojni cilj ne može napraviti za kibernetički prostor ili internetsku infrastrukturu općenito.[93] Umjesto toga, zaraćene stranke moraju identificirati točno određene dijelove interneta koji se koriste u vojne svrhe, pa kao takvi mogu postati vojni cilj. Sličnog je stajališta i Tallinnski priručnik 2.0 koji smatra da bi gotovo svaki napad na internet trebao biti ograničen isključivo na njegove zasebne segmente.[94] Upravo visoka specijaliziranost kibernetičkih sredstava napada otvara mogućnost da ti napadi budu usmjereni na točno određene dijelove internetske infrastrukture kao vojnog cilja, te da se poduzmu sve moguće mjere opreza kako bi se izbjegao ili barem minimizirao negativan utjecaj na ostale dijelove internetske infrastrukture. Ipak, takvi napadi koji ciljaju cjelokupan internet su zasad samo teoretsko pitanje jer, kako Tallinnski priručnik 2.0 navodi: "*okolnosti pod kojima bi internet u cijelosti mogao biti napadnut su malo vjerojatne*".[95]

5.1.1.2. Računalni podaci kao objekti

Mogu li se računalni podaci smatrati objektom u smislu Protokola I. i kao takvi uživati jednaku zaštitu koju imaju i ostali civilni objekti? Kao što je ranije rečeno, ako su računalni podaci meta napada koji uzrokuje smrt ili ozljedu osobe odnosno štetu ili gubitak funkcionalnosti fizičkog objekta, takva kibernetička operacija bit će napad neovisno od toga smatraju li se računalni podatci objektima. U tom slučaju, računalni podatci uživaju zaštitu

[91] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 101, str. 446.
[92] *Ibid.* str. 447.
[93] Dormann; Laurent, *op. cit.* (bilj. 44), str. 321.
[94] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 101, str. 445.
[95] *Ibid.*

koju im pruža međunarodno humanitarno pravo. No, pitanje mogu li se računalni podatci smatrati objektom je ključno za one kibernetičke operacije koje neće izazvati takve posljedice.

Mišljenja mogu li se računalni podatci smatrati objektom su trenutno podijeljena. Većina međunarodne skupina stručnjaka smatra da se podaci ne bi mogli smatrati objektom.[96] Svoje stajalište temelje na tome da MOCK opisuje objekt kao nešto što je "*materijalno, vidljivo i opipljivo*", a računalni podaci, kakvi postoje u kibernetičkom prostoru, to definitivno nisu.[97] Također, ukoliko se pojam objekta tumači u skladu s člankom 31. Bečke konvencije o pravu međunarodnih ugovora, obično značenje pojma objekt tada ne bi uključivalo računalne podatke.[98]

No, treba uzeti u obzir što sve računalni podaci uključuju. Danas države medicinske podatke, podatke o oporezivanju i popise stanovništva, imaju kako u fizičkom tako i u digitalnom obliku, a u nekim slučajevima i isključivo u digitalnom obliku. Gubitak takvih digitaliziranih podataka predstavljao bi veliki udarac za državu te izazvao puno veće poteškoće u obavljanju temeljnih državnih funkcija nego što bi to bilo u slučaju uništenja fizičkih ekvivalenti takvih podataka. Uzimajući to u obzir, drugo mišljenje, koje zastupa MOCK, je da su računalni podaci objekti prema međunarodnom humanitarnom pravu. MOCK navodi da "*Zaključak da ovu vrstu operacije ne bi zabranilo međunarodno humanitarno pravo u današnjem svijetu koji se sve više oslanja na kibernetičku tehnologiju – bilo zato što brisanje ili neovlašteno mijenjanje takvih podataka ne bi predstavljalo napad u smislu međunarodnog humanitarnog prava ili zato što se takvi podaci ne bi smatrali predmetom koji bi spadao pod zabranu napada na civilne objekte – čini se teško pomirljivim s ciljem i svrhom ovog skupa normi".*[99]

Unatoč tome, nijedan od ranije navedenih pristupa ne može se smatrati dovoljno zadovoljavajućim. Restriktivan pristup Tallinnskog priručnika 2.0 nedovoljno je uključiv, jer ostavlja mogućnost da računalni podatci budu uništeni ili izmijenjeni. To bi moglo imati ozbiljne posljedice za civilno stanovništvo te bi bilo u suprotnosti s ciljem i svrhom međunarodnog humanitarnog prava. Nasuprot tome, shvaćanje da se računalni podatak sam po sebi smatra objektom pod zaštitom međunarodnog humanitarnog prava je previše uključiv.

[96] *Ibid.*, Commentary on Rule 100, str. 436.
[97] Sandoz, Yves; Swinarski, Christophe; Zimmerman, Bruno (ur.), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ICRC, Geneva, 1987 (ICRC Commentary on the APs), paragraf 2008.
[98] Bečka konvencija o pravu međunarodnih ugovora, 1969, Narodne novine, Međunarodni ugovori, 13/1993, čl.31(1).
[99] International humanitarian law and the challenges of contemporary armed conflicts - Report, *op. cit.* (bilj. 22), str. 43.

Države bi teško prihvatile takvo shvaćanje koje bi im onemogućilo provođenje kibernetičkih napada na sve računalne podatke.

Potpuno rješenje tog pitanja moći će biti postignuto samo konsenzusom država i preciznim definiranjem pojma računalnih podataka. Ipak, s obzirom da se takvo razjašnjenje ne očekuje u bližoj budućnosti, postoje određeni prijedlozi kako riješiti ili barem minimalizirati takav problem.[100] Michael N. Schmitt predlaže da se zaštita pruži bitnim civilnim funkcijama ili uslugama a ne računalnim podatcima.[101] Države bi trebale "*dati posebnu zaštitu određenim bitnim civilnim funkcijama ili uslugama obvezujući se suzdržati se od provođenja kibernetičkih operacija protiv civilne infrastrukture ili podataka koji ih ometaju*".[102] Tako bi se pitanje može li se određeni računalni podatak smatrati objektom zaobišlo, a težina bi se stavila na važnost usluge ili funkcije za civilnu populaciju. Na takav način stvorio bi se balans između dva mišljenja, stavljajući u prvi plan zaštitu civilne populacije i civilnih objekata, a istovremeno poštujući i trenutno stajalište da se pojam objekta previše ne širi.

5.1.2. Osobe

Jedan od glavnih zadataka međunarodnog humanitarnog prava je zaštititi civilno stanovništvo od učinaka oružanog sukoba. Jednako kao i kod objekata, stranke u sukobu mogu napadati samo one osobe koje se mogu smatrati vojnim ciljem, a koje uključuju ponajprije borce, zatim članove organiziranih naoružanih skupina i konačno one civile koji izravno sudjeluju u neprijateljstvima. Civilima je zabranjeno izravno sudjelovati u neprijateljstvima i ako u njima sudjeluju gube zaštitu od napada. Zbog specifičnosti kibernetičkih operacija postoje određene poteškoće u primjeni tih pravila. Kako čimbenike koji su relevantni za status borca, poput podvrgnutosti zapovjedništvu i unutrašnjem disciplinskom sustavu, treba tumačiti u kibernetičkom prostoru, gdje osobe mogu djelovati kolektivno bez međusobne povezanosti ili hijerarhijske zapovjedne strukture? Kako zbog povezanosti civilne i vojne infrastrukture razlikovati civile od boraca? Imaju li civili pravo na zaštitu ako sudjeluju samo u izradi ili održavanju kibernetičkih sredstava? Navedena pitanja trebaju biti razjašnjena kako bi civili izloženi kibernetičkim napadima mogli dobiti zaštitu koju im pruža međunarodno humanitarno pravo.

---

[100] *v. npr*: Dinniss, Harrison, Heather, A., "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", Israel Law Review, Vol. 48/2015; Mačák, Kubo, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", Israel Law Review, Vol. 58/2015.

[101] Schmitt, Michael, N., "Wired warfare 3.0: Protecting the civilian population during cyber operations", International Review of the Red Cross, Vol. 101/2019, str. 345.

[102] *Ibid.*

5.1.2.1. Tko može izvršiti kibernetički napad?

Da bi napad mogao biti ograničen samo na one osobe koje sudjeluju u neprijateljstvima, potrebno je da se te osobe po nekom znaku razlikuju od ostalih, ponajprije civila. Ženevske konvencije iz 1949. godine, koje su i dalje na snazi za one države koje nisu stranke Protokola I., navode da se osobe mogu smatrati borcem ako im na čelu stoji odgovoran zapovjednik, ako nose određeni i vidljivi znak raspoznavanja, ako otvoreno nose oružje, te ako se pridržavaju pravila ratnog prava.[103] Samo takve osobe mogu izvoditi napade.

Protokol I. dodatno je proširio definiciju pojma oružanih snaga. Protokol I. određuje da se pripadnici oružanih snaga stranke sukoba smatraju borcima[104], te da se oružane snage sastoje od svih organiziranih oružanih snaga, naoružanih grupa i jedinica koje su pod zapovjedništvom odgovornim toj stranci.[105] Nadalje, oružane snage moraju biti podvrgnute unutrašnjem disciplinskom sustavu, koji uz ostalo, osigurava poštivanje pravila međunarodnog humanitarnog prava.[106] Također, moguće je tvrditi da su u zahtjevu da se oružane snage podvrgnu unutrašnjem disciplinskom sustavu sadržani i zahtjevi nošenja određenog i vidljivog znaka raspoznavanja i otvorenog nošenja oružja.[107] Prema tome, da bi se dobio status borca potrebno je da je ispunjen zahtjev postojanja zapovjedništva odgovornog stranci sukoba te da su oružane snage podvrgnute unutrašnjem disciplinskom sustavu.

Definicija borca se može primijeniti na slučajeve kada država provodi kibernetičke napade uporabom svojih oružanih snaga gdje postoji određena razina organizacije i zapovjedne odgovornosti. No, država se može obratiti i skupini privatnih osoba za provođenje kibernetičkih operacija tijekom oružanog sukoba jer takva skupina posjeduje sposobnost ili znanje koje državni organi nemaju.[108] Takve skupine dobivaju implicitni pristanak te ponekad čak i upute države za djelovanje u svojim kibernetičkim napadima.[109] Još jedna prednost korištenja takvih skupina za izvođenje kibernetičkih napada je vrlo lako maskiranje umiješanosti države u napad. Slična situacija se dogodila za vrijeme kibernetičkih napada na Estoniju 2007. godine kada je Nashi, pro-ruska skupina bliska vlastima, preuzela odgovornost za napade.[110] Tallinnski priručnik 2.0 navodi da će se, sve dok takve skupine pripadaju stranci

[103] *v.* čl. 13. Ženevske konvencije za poboljšanje položaja ranjenika i bolesnika u oružanim snagama u ratu 1949, i Ženevske konvencije za poboljšanje položaja ranjenika, bolesnika i brodolomaca oružanih snaga na moru 1949, te čl. 4. Ženevske konvencije o postupanju s ratnim zarobljenicima 1949.
[104] Protokol I., *op. cit.* (bilj. 29), čl. 42(2).
[105] *Ibid.* čl. 43(1).
[106] *Ibid.*
[107] Andrassy, Bakotić, Seršić, Vukas, *op. cit.* (bilj. 8), str. 142.
[108] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 87, str. 403.
[109] Gervais, Michael, "Cyber Attacks and the Laws of War", Journal of War & Cyber Warfare, Vol. 1/2012, str. 36.
[110] Hathaway, O. A. *et. al*., *op*. cit. (bilj. 23), str. 41-42.

u sukobu i sve dok ispunjavaju ostale uvjete, njihovi članovi smatrati borcima i kao takvi moći biti meta napada.[111] Ipak, definiciju borca prema međunarodnom humanitarnom pravu teško je u potpunosti primijeniti u kibernetičkom prostoru, gdje zbog sve veće dostupnosti kibernetičkih sredstava, neorganizirani pojedinci zbog patriotskih ili ideoloških razloga također mogu sudjelovati u kibernetičkim napadima na protivnika.[112] S obzirom da se danas sve velike hakerske skupine isključivo organiziraju putem interneta a zapovjedna hijerarhija im je fragmentirana a nekad i nepostojeća, može doći do poteškoća u utvrđivanju zahtjeva djelovanja pod zapovjedništvom odgovornim stranci sukoba. U tom slučaju zahtjev da skupina bude podvrgnuta unutrašnjem disciplinskom sustavu koji može osigurati poštivanje pravila međunarodnog humanitarnog prava još je teže ispuniti. Zbog toga je vrlo malo vjerojatno da bi se hakerska skupina koja djeluje u kibernetičkom prostoru mogla kvalificirati kao organizirana oružana skupina u svrhu određivanja statusa borca.[113]

U zahtjevu da se oružane snage podvrgnu unutrašnjem disciplinskom sustavu sadržani su i zahtjevi da otvoreno nose oružje i koriste znakove raspoznavanja.[114] Zahtjev da osoba nosi znak raspoznavanja općenito se smatra ispunjenim nošenjem uniformi. Tallinnski priručnik 2.0 navodi kako ne postoji osnova za odstupanje od navedenog zahtjeva za one osobe koje provode kibernetičke operacije.[115] Iako je jedan dio stručnjaka smatrao da te osobe bez obzira na okolnosti poput udaljenosti od bojišta ili jasnog odvajanja od civilnog stanovništva moraju uvijek ispunjavati ovaj zahtjev kako bi uživali status borca, drugi su smatrali kako se taj zahtjev primjenjuje samo u okolnostima u kojima ne nošenje uniforme može prouzročiti da napadač ne može razlikovati civile od boraca, čime bi civili bili izloženi većem riziku od napada.[116] U pogledu zahtjeva za otvorenim nošenjem oružja Tallinnski priručnik 2.0 smatra kako bi takav zahtjev ima malo primjene u kibernetičkom prostoru.[117] Zbog činjenice da sveukupne posljedice kibernetičkog napada mogu biti poznate tek kasnije kao i zbog toga da se osobe koje te napade izvode često nalaze daleko od bojišnice to pravilo bi bilo teško primijeniti na kibernetičke operacije.

[111] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 87, str. 403.
[112] Gervais, *op. cit.* (bilj. 109), str. 34.
[113] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 87, str. 403.
[114] Andrassy, Bakotić, Seršić, Vukas, op. cit. (bilj. 8), str. 142.
[115] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 87, str. 403.
[116] *Ibid.*, Commentary on Rule 87, str. 405.
[117] *Ibid.*

5.1.2.2. Tko može biti meta kibernetičkih napada?

Jedna od svrha pravila razlikovanja je ta da zaraćene stranke u borbi ciljaju borce a ne civile. Odredbe međunarodnog humanitarnog prava propisuju da zakonito ciljani mogu biti samo borci, članovi organiziranih naoružanih skupina i civili koji izravno sudjeluju u neprijateljstvima. Tallinnski priručnik 2.0 navodi da civilno stanovništvo, kao ni pojedinačni civili, ne smiju biti predmetom kibernetičkog napada.[118]

Ako postoji sumnje je li osoba civil, ta osoba će se smatrati civilom. Zbog prirode kibernetičkog prostora i načina na koji se kibernetički napadi provode, sumnja u status osobe može biti vrlo česta pojava. Kao što je već ranije navedeno, veliki dio kibernetičke infrastrukture koristi se kako od strane civila tako i od vojske, dok, s obzirom na povezanost sustava u kibernetičkom prostoru, mreže koje koriste civili i oružane snage mogu biti međusobno povezane. U takvim slučajevima, korištenje računala ili korištenje određene mreže, pa čak i ako se ona može kvalificirati kao vojna, ne mora samo po sebi značiti da osoba nije civil.[119]

Nadalje, pravilo je međunarodnog humanitarnog prava da civili gube svoje pravo da ne budu meta napada ukoliko izravno sudjeluju u neprijateljstvima.[120] Ukoliko osoba izvede kibernetički napad na način da prikuplja informacije o neprijateljskim operacijama pomoću kibernetičkih sredstva ili provodi DoS napade (*eng. denial of service attacks*)[121] protiv neprijateljskih vojnih sustava tada ta osoba gubi svoju zaštitu.[122] No, što je sa civilnim programerima koji sudjeluju samo u dizajnu ili održavanju kibernetičkih sredstava, kao na primjer zlonamjernog softvera, te mogu li i oni biti meta napada? Prema jednom mišljenju, postupci takvog civila mogli bi se smatrati "*kontinuiranom funkcijom koja uključuje pripremu, izvršenje ili zapovijedanje radnjama ili operacijama koje predstavljaju izravno sudjelovanje u neprijateljstvima*"[123] čime bi se navedeni programer mogao smatrati zakonitom metom napada. S druge strane, Tallinski priručnik 2.0 navodi kako dizajniranje ili održavanje zlonamjernog softvera ne bi predstavljalo izravno sudjelovanje u neprijateljstvima.[124]

---

[118] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Rule 94, str. 422.
[119] *Ibid.*, Rule 95, str 423.
[120] Protokol I., *op. cit.* (bilj. 29), čl. 51(3).
[121] Izraz DoS napad označava napad uskraćivanja usluga. Takav napad karakterizira namjerno slanje velike količine mrežnog prometa što rezultira preopterećenjem mrežnih resursa i poslužitelja te dovodi do nemogućnosti pružanja usluga. *v. više*. CARNet CERT, DDoS napad, Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-09-240.pdf (27.10.2023).
[122] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 87, str. 403.
[123] Melzer, Niels, Interpretative guidance on the notion of direct participation in hostilities under international humanitarian law, ICRC, 2009, str. 34.
[124] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 97, str. 429.

5.1.3. Neselektivne kibernetičke metode i sredstva i neselektivni kibernetički napadi

Zabrana neselektivnih metoda i sredstava te neselektivnih napada proizlazi iz pravila razlikovanja.[125] Neselektivni napadi su oni koji su toliko neprecizni da rezultiraju kolateralnom štetom.[126] Protokol I. definira tri vrste neselektivnih napada: (1) napadi koji nisu usmjereni na određeni vojni cilj; (2) napadi koji koriste metode ili sredstva ratovanja koja se ne mogu usmjeriti na određeni vojni cilj; i (3) napadi koji koriste metode ili sredstva ratovanja čije se posljedice ne mogu ograničiti.[127] Kao što je naveo Međunarodni sud, stranke u sukobu "*nikada ne smiju koristiti oružje koje nije u stanju razlikovati civilne od vojnih ciljeva*".[128] Prema tome, neselektivno je oružje, poput biološkog ili kemijskog oružja, zabranjeno.

Slična situacija postoji i u sferi kibernetičkih operacija. Ukoliko se kibernetički napad izvodi neselektivnim kibernetičkim sredstvom, zbog povezanosti sustava u kibernetičkom prostoru, postoji velika opasnost da osim vojnih objekata budu ugroženi i civilni. Kibernetička sredstva napada često je teško kontrolirati, pa stoga njihovi učinci mogu biti neselektivni.[129] Pa bi tako korištenje računalnog crva koji se sam replicira i nije pod kontrolom napadača, te bi stoga mogao uzrokovati značajnu štetu civilnoj infrastrukturi tako što nenamjerno zarazi milijune računala u pokušaju da se aktivira na jednoj ciljanoj mreži, bila povreda međunarodnog humanitarnog prava. Ako se repliciranje ili opseg sustava koji je meta kibernetičkog napada ne može ograničiti onda je takvo kibernetičko sredstvo neselektivno i zabranjeno.[130] Također, međunarodno humanitarno pravo zabranjuje i razvoj kibernetičkih oružja koja bi bila neselektivna ili bi bila takve prirode da uzrokuju suvišne ozljede ili nepotrebnu patnju.[131] Korištenje takvog oružja treba zabraniti odmah prilikom njegovog razvoja ili nabave.[132] Osim toga, prije svakog planiranog napada, napadač mora provjeriti može li kibernetičko oružje biti i je li ono usmjereno na vojni cilj te mogu li učinci takvog kibernetičkog oružja biti kontrolirani.[133] S druge strane, uporaba kibernetičkih sredstava koja imaju neselektivne učinke isključivo zbog nepredvidivog kvara sustava ne smatra se neselektivnom.[134]

---

[125] MOCK, Customory IHL - Rules, Rule 12, Dostupno na: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule10#Fn_A84730F9_00002 (26.9.2023).
[126] Gervais, *op. cit.* (bilj. 109), str. 36.
[127] Protokol I., *op. cit.* (bilj. 29), čl. 51(4).
[128] ICJ, *op. cit*. (bilj. 33), paragraf 78.
[129] Gervais, *op. cit.* (bilj. 109), str. 43.
[130] Pascucci, *op. cit*. (bilj. 27), str. 440.
[131] Dormann; Laurent, *op. cit.* (bilj. 44), str. 301.
[132] Droege, *op. cit.* (bilj. 50), str. 571.
[133] *Ibid.*
[134] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 105, str. 456.

Ipak nije svako kibernetičko oružje nužno neselektivno. Moguće je dizajnirati kibernetičko oružje na način koji dopušta njegovo djelovanje samo prema točno određenim vojnim ciljevima.[135] U tom slučaju, s obzirom da kibernetičko sredstvo dopušta precizno ciljanje, napadači moraju koristiti to sredstvo na način da ga upotrebe protiv vojnih, a ne civilnih ciljeva. Tallinski priručnik 2.0 daje primjer virusa namijenjenog da ošteti sustave u vojnoj bazi, ali se širi putem USB *sticka* ostavljenog na raznim konferencijama u nadi da će se na kraju koristiti u spomenutoj vojnoj bazi.[136] U tom slučaju, kibernetičko sredstvo napada je selektivno, ali je sam napad neselektivan. Iako je danas izrada visokospecijaliziranih selektivnih kibernetičkih sredstava moguća, to nije jamstvo da će u konačnici ono takvo i biti - iako dizajniran da djeluje samo na iranska nuklearna postrojenja, Stuxnet je zarazio računala i u ostalim državama diljem svijeta.[137] Zbog toga napadač veliku pažnju treba usmjeriti na pripremu i planiranje napada kao i na odabir odgovarajuće metode i sredstva.

5.2. PRAVILO PROPORCIONALNOSTI

Jednom kada je napadač izvršio razlikovanje između vojnih i civilnih objekata te kada su vojni ciljevi napadnuti, civili i civilni objekti moraju biti pošteđeni od slučajne ili kolateralne štete u najvećoj mogućoj mjeri. Ukoliko dođe do slučajne ili kolateralne štete ona ne smije biti pretjerana u odnosu na predviđenu stvarnu i izravnu vojnu prednost koju napadač očekuje od svojeg napada - to je pravilo proporcionalnosti.[138]

Pravilo proporcionalnosti služi kao dopuna zabrani neselektivnih napada, te je osmišljeno kako bi se pojačala zaštita koju pruža načelo razlikovanja.[139] Ono zabranjuje "*napad od kojeg se može očekivati da će prouzročiti slučajne gubitke života među civilnim stanovništvom, ranjavanje građanskih osoba, štete na civilnim objektima ili kombinaciju toga, što bi bilo prekomjerno u odnosu na predviđenu stvarnu i izravnu vojnu prednost*".[140] Osim što takav napad zabranjuje međunarodno humanitarno pravo i Rimski statut Međunarodnog

[135] Mayuko, Torii, "Issues concerning Cyber Attacks in Light of the Law of Armed Conflict", Air and Space Power Studies, Vol. 7, str. 267. Dostupno na https://www.mod.go.jp/asdf/meguro/center/Eimg/10aspw7.pdf (27.9.2023).
[136] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 111, str. 467.
[137] Iako je Stuxnet zarazio civilne industrijske sustave upravljanja diljem svijeta, nije uzrokovao nikakva oštećenja jer je dizajniran na takav način da može djelovati destruktivno samo kada se otkrije točno određena konfiguracija računala. Takva konfiguracija nalazila se samo u iranskoj nuklearnoj elektrani Natanz. Zbog toga bi Stuxnet zadovoljavao kriterije razlikovanja jer je dizajniran samo za određeni vojni cilj i nije mogao neselektivno napadati civilne sustave.
[138] MOCK, Introduction to the Law of Armed Conflict, 2002, str. 13-1 Dostupno na: https://www.icrc.org/en/doc/assets/files/other/law1_final.pdf ghfg (27.9.2023).
[139] Pascucci, *op. cit*. (bilj. 27), str. 445.
[140] Protokol I., *op. cit.* (bilj. 29), čl. 51(5)(b).

kaznenog suda navodi neproporcionalne napade poput „*opsežnog uništavanja i oduzimanja imovine koje nije opravdano vojnim potrebama i koje je provedeno nezakonito i samovoljno*"[141] te "*namjernog pokretanja napada sa znanjem da će takav napad uzgredno dovesti do smrti ili ozljeda civila ili štete na civilnim objektima ili do teške, dugoročne i opsežne štete u prirodnom okolišu koja bi očito bila prevelika u odnosu na očekivani konkretan i izravan vojni dobitak"* i klasificira ih kao ratne zločine.[142] Stoga je vrlo bitno da napadači poštuju pravilo proporcionalnosti pri provođenju kibernetičkih napada.

Pravilo proporcionalnosti ograničava stupanj i vrstu sile koja se koristi za postizanje vojnog cilja tako što uspoređuje predviđenu stvarnu i izravnu vojnu prednost s očekivanom slučajnom štetom za civile i civilnu imovinu.[143] Bitno je napomenuti da nije svaki napad koji za posljedicu ima smrt civila ili uništavanje civilne imovine povreda pravila proporcionalnosti. Općenito je prihvaćeno da postoje određene granice proporcionalnosti unutar kojih zapovjednik ima diskrecijsko pravo djelovati.[144] Prema tome, određeni stupanj kolateralne štete ipak je dopušten, ali samo ako je očekivana kolateralna šteta razmjerna u usporedbi s očekivanom vojnom prednošću. Ono što je prema načelu proporcionalnosti definitivno zabranjeno je napad koji je bezobziran ili napad koji svjesno oduzima živote civila ili uništava imovinu civila više nego što je potrebno za postizanje vojnog cilja.

Prema Tallinskom priručniku 2.0 pravilo proporcionalnosti također je primjenjivo i na kibernetičke operacije.[145] Da bi napadač pravilno proveo test proporcionalnosti, on mora provesti analizu potencijalnih civilnih žrtava i uništenja civilne imovine i usporediti ih s očekivanom korišću postizanja vojne prednosti. No, zbog specifičnosti kibernetičkih napada i prirode štete koju oni nanose, ta analiza proporcionalnosti otvara potencijalne probleme.

Jednako kao i kod pravila razlikovanja i ovdje će biti potrebno odrediti u kojoj mjeri pojam "šteta" obuhvaća gubitak funkcionalnosti.[146] S obzirom da je takvoj civilnoj infrastrukturi potrebno pružiti odgovarajuću zaštitu, nema zapreke tomu da se, jednako kao i kod razlikovanja, šteta od kibernetičkog napada smatra ne samo fizičkom štetom, već i gubitkom funkcionalnosti civilne kibernetičke infrastrukture čak i u odsutnosti bilo kakve fizičke štete.

---

[141] Rimski statut Međunarodnog kaznenog suda, *op. cit*. (bilj. 65), čl. 8(2)(a)(iv).
[142] *Ibid,* 8(2)(b)(iv).
[143] Gervais, *op. cit.* (bilj. 109), str. 38.
[144] *v. više*. Final Report to the Prosecutor by the committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, 2003. Dostupno na: https://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal (27.9.2023).
[145] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Rule 113, str. 470.
[146] Diamond, Eitan, *op. cit*. (bilj. 78), str. 79.

Nadalje, kod primjene pravila proporcionalnosti osobitu pažnju treba obratiti na objekte dvojne namjene. Da bi se mogao izvršiti napad na objekte dvojne namjene takav objekt mora proći test proporcionalnosti, odnosno šteta koja može nastati njegovim uništenjem ne smije biti pretjerana u odnosu na predviđenu stvarnu i izravnu vojnu prednost napadaču. Iako se, kao što je ranije rečeno, objekti dvojne namjene mogu smatrati vojnim ciljem, činjenica da takvu infrastrukturu koriste i civili komplicira primjenu pravila proporcionalnosti. S obzirom da je, zbog njihove međusobne povezanosti, teško razaznati civilnu od vojne kibernetičke infrastrukture, postoji velika mogućnost da napad na takvu infrastrukturu dovede do kolateralne štete. To bi značilo da će pretpostavljena kolateralna šteta izračunata u testu proporcionalnosti biti daleko veća od stvarne i izravne vojne prednosti. Odnosno, povećana vjerojatnost kolateralne šteta onemogućila bi predloženom kibernetičkom napadu da prođe test proporcionalnosti.[147]

Isto tako, kod primjene pravila proporcionalnosti na kibernetičke napade postoji određena neizvjesnosti o tome što se može smatrati potencijalnom kolateralnom štetom na civilnim objektima.[148] Potencijalna kolateralna šteta, može se sastojati od izravnih i neizravnih učinaka. Iako je odgovornost napadača da prvenstveno pazi na izravne učinke, prisutnost neizravnih učinaka koji proizlaze iz određene radnje, ali se ne mogu odmah uočiti dodatno komplicira situaciju. Neizravni učinci mogu se definirati kao "*neizravne posljedice koje proizlaze iz izravnih rezultata određene akcije*".[149] Prema tome, neizravni učinci kibernetičkog napada sastojali bi se od "*odgođenih i/ili pomaknutih posljedica djelovanja drugog, trećeg i višeg reda, stvorenih preko posrednih događaja ili mehanizama*".[150] Kibernetički napadi su relativno nova metoda ratovanja te se malo zna o njihovim potencijalnim učincima. Tipični učinci kibernetičkih napada mogu biti nesmrtonosni ili samo privremeni.[151] Isto tako, zbog već ranije spomenute međusobne povezanosti kibernetičkih sustava, teško je utvrditi točan učinak kibernetičkih napada i odrediti kako takvi napadi mogu utjecati na stvari ili objekte koji nisu bili početna meta napada.[152] Na primjer, ako je došlo do blokade ili poremećaja GPS-a uzrokovanih kibernetičkim napadom kratkoročno se mogu očekivati nesreće koje uključuju

[147] Fenton, *op. cit*. (bilj. 70), str 349.
[148] Droege, *op. cit.* (bilj. 49), str. 572.
[149] Jensen, Eric, T., "Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?", American University International Law review, Vol.18/2003. Dostupno na: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1208&context=auilr (27.9.2023).
[150] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 113, str. 471.
[151] Hathaway, O. A. *et. al*., *op*. cit. (bilj. 23), str. 38.
[152] Diamond, Eitan, *op. cit*. (bilj. 78), str. 79.

transportna sredstva koja se oslanjaju na navigacijske podatke koje taj sustav pruža.[153] Također, s obzirom na međusobnu povezanost kibernetičkih sustava, moguće je da svi učinci takvog kibernetičko napada napadaču neće biti niti poznati. Tallinnski priručnik 2.0 navodi da kolateralna šteta koja se uzima u obzir u analizi proporcionalnosti "*uključuje sve neizravne učinke koje bi trebali očekivati pojedinci koji planiraju, odobravaju ili provode kibernetički napad*".[154] Kao primjer se uzima napadač koji može odlučiti umetnuti virus u određeni vojni računalni sustav koji ne samo da će onemogućiti taj sustav, već će se vjerojatno proširiti na ograničen broj civilnih računalnih sustava, uzrokujući na taj način kolateralnu štetu. Prema Tallinskom priručniku 2.0 ti se učinci, ako se jesu ili su se trebali očekivati, moraju uzeti u obzir pri provođenju testa proporcionalnosti. Odnosno, može se zaključiti da se predvidive štete, čak i ako su odgođene i/ili pomaknute štete drugog i trećeg i višeg reda, moraju uzeti u obzir.[155] No, ako se isti virus prenese na civilne računalne sustave nekim drugim putem koji je bio neočekivan ili nepredvidiv tada se posljedice koje iz toga proizlaze neće uzeti u obzir prilikom testa proporcionalnosti.

Treba napomenuti i to da bi napad na neke objekte imao tako opasne neizravne učinke da je njihovo ciljanje već *a priori* potpuno zabranjeno. Kako Protokol I. navodi, „*Postrojenja ili instalacije koje sadrže opasne sile, to jest brane, nasipi i nuklearne elektrane, neće biti predmet napada čak ni kad su vojni ciljevi, ako takvi napadi mogu prouzročiti oslobađanje tih sila i posljedično velike gubitke među civilnim stanovništvom*".[156] Nema zapreke da se navedena zabrana odnosi i na zabranu izvođenja kibernetičkih napada.

S druge strane, jedna od prednosti kibernetičkih napada je ta što dopuštaju napadaču da, ukoliko to želi, u najvećoj mogućoj mjeri smanji mogućnost kolateralne štete. Visoka sofisticiranost kibernetičkih sredstava i mogućnost da budu upotrijebljeni na točno određene mete omogućili bi lakše poštivanje pravila proporcionalnosti od uporabe tradicionalnog kinetičkog oružja. Na primjer, u slučaju postojanja aktivnih obrambenih mjera osmišljenih da napadnu samo računalni sustav s kojeg kibernetički napad potječe i tako zaustave napad, osigurat će se da te mjere ciljaju samo izvor kibernetičkog napada a ne i ostale sustave.[157] Također, uporabom informacijskih tehnologija moderno streljivo može biti precizno navođeno te se tako kolateralnu štetu koja može proizaći iz napada može značajno smanjiti.[158] Osim toga,

[153] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 113, str. 471.
[154] *Ibid.*
[155] Geiss; Lahmann, *op. cit*. (bilj. 82), str 16.
[156] Protokol I., *op. cit.* (bilj. 29), čl. 56.
[157] Graham, D. E., "Cyber Threats and the Law of War", Journal od National Security and Policy, Vol. 4/2010, str. 89.
[158] Lin, *op. cit*. (bilj. 11), str. 546.

kibernetički napad je potencijalno reverzibilan, pa ukoliko su učinci veći od očekivanih ostavlja se mogućnost napadaču da napad prekine.[159] Takav napad smanjio bi mogućnost kolateralne štetu u odnosu na onu koja bi proizašla iz uporabe tradicionalnog kinetičkog oružja, čime bi se pomoglo u postizanju proporcionalnosti. Korištenje takvih kibernetičkih sredstava mogla bi biti preferirana metoda za one države koje žele primijeniti razmjernu razinu sile, ali pritom pazeći na živote i imovinu civila.[160]

Pravilna primjena pravila proporcionalnosti, kako kod kinetičkih tako i kod kibernetičkih napada je teška. Od svih pravila međunarodnog humanitarnog prava, pravilo proporcionalnosti je "*među najsloženijim i najneshvaćenijim u pogledu tumačenja i primjene*".[161] Osim što se mora voditi računa o ranije izloženim problemima napadač se mora prilikom izvođenja kibernetičkog napada držati i dodatnih pravila. Prvenstveno, test proporcionalnosti treba biti proveden *ex ante* a ne *ex post*.[162] Pravilna primjena proporcionalnosti zahtijeva procjenu razumnosti odluke napadača u vrijeme kada je napad planiran, odobren ili izvršen, a ne nakon toga.[163] Prilikom planiranja kibernetičkog napada napadač treba uzeti u obzir vrijednost ciljane mete, je li napad nudio dovoljno jasnu vojnu prednost te je li izveden imajući na umu zaštitu života i imovine civila.[164] Također, pri planiranju, odobrenju i izvršenju kibernetičkih napada, sve naizgled pouzdane informacije koje su dostupne moraju se uzeti u obzir. Loše planiranje zapovjednika, nedovoljno dobar obavještajni rad i kontrola ciljeva lako mogu rezultirati uništenjem civilnih objekata i smrću civilnog stanovništva.[165] Međunarodni kazneni sud za bivšu Jugoslaviju bavio se pitanjem razumnosti konačne odluke o proporcionalnosti u presudi Galić te je zaključio da "*Prilikom utvrđivanja je li napad bio razmjeran, potrebno je ispitati je li razumno dobro obaviještena osoba, uz razumno korištenje informacija koje su joj bile dostupne, mogla očekivati prekomjerne civilne gubitke koji bi bili posljedica napada*".[166] Nema zapreke da se taj isti standard primijeni i na kibernetičke napade. U svakom slučaju napadač bi u većini slučajeva trebao očekivati kolateralnu štetu, čak i ako je njen točan opseg teško procijeniti.[167] Konačno,

[159] Gervais, *op. cit.* (bilj. 109), str. 39.
[160] *Ibid.*
[161] Schmitt, Michael N., „Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics", Harvard National Security Journal, 2013, str. 18.
[162] Pascuci, *op. cit.* (bilj. 27), str 445-446.
[163] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 113, str. 473.
[164] Gervais, *op. cit.* (bilj. 109), str. 40.
[165] MOCK, *op. cit.* (bilj. 138) str 13-1.
[166] ICTY, Prosecutor v. Stanislav Galić, Trial Chamber judgment, 2003, paragraf 58. Dostupno na https://www.icty.org/x/cases/galic/tjug/en/ (27.9.2023).
[167] Schmitt, Michael, N; O'Donnel, Brian T., "Computer Network Attack and International Law", International Law Studies, Vol. 76/2002, str. 169.

treba napomenuti da se, jednako kao i kod pravila razlikovanja, test proporcionalnosti kibernetičkog napada uvijek mora razmatrati od slučaja do slučaja.[168]

5.3. MJERE OPREZA

Prije poduzimanja napada, potrebno je poduzeti određene mjere opreza. Pravilo poduzimanja mjera opreza dio je običajnog međunarodnog prava i kodificirano je u člancima 57. i 58. Protokola I. Ono služi kao dopuna pravilima razlikovanja i proporcionalnosti.[169] Međunarodno humanitarno pravo zahtijeva od zaraćenih stranaka da poduzmu mjere opreza prilikom napada, kao i mjere opreza u odnosu na posljedica napada.[170]

5.3.1. Mjere opreza prilikom napada

Osnovno pravilo međunarodnog humanitarnog prava je da vojne operacije moraju biti usmjerene isključivo na vojne ciljeve te se stoga mora stalno voditi računa da se poštedi civilno stanovništvo ili civilni objekti. To osnovno pravilo dopunjeno je posebnim pravilima koja uključuju poduzimanje svih mogućih mjera kako bi se potvrdilo da su mete uistinu vojni ciljevi kao i poduzimanje svih mogućih mjera opreza u odabiru sredstava i metoda ratovanja s ciljem izbjegavanja i minimiziranja slučajnih civilnih žrtava i štete na civilnim objektima. Također, zahtijeva se da stranke u sukobu otkažu ili obustave napad ako postane očito da će takav napad uzrokovati pretjeranu kolateralnu štetu.[171] Prema tome, mjere opreza bi mogle uključivati obvezu kao što je prikupljanje svih dostupnih informacija za provjeru cilja i mogućih slučajnih učinaka napada.[172] Ti preventivni koraci bi osigurali da niti jedan civil ili civilni objekt ne budu ciljani tijekom napada.

U kontekstu kibernetičkih operacija, napadač bi trebao učiniti sve što je moguće kako bi pribavio informacije potrebne za provjeru je li odabrana meta vojni cilj i kako bi se uvjerio da napad neće uzrokovati pretjeranu kolateralnu štetu. Takva dužnost je konstantna, što znači da ne postoji samo prilikom pripreme operacije, već i dok je ona u tijeku.[173] Ako su dostupne

[168] Gervais, *op. cit.* (bilj. 109), str. 40.
[169] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 114, str. 476
[170] Protokol I., *op. cit.* (bilj. 29), čl. 57 i 58.
[171] Protokol I., *op. cit.* (bilj. 29), čl. 57(2)(b).
[172] ICTY, Final Report to the Prosecutor, paragraf 29; U svom završnom izvješću, Odbor osnovan za reviziju NATO-ove kampanje bombardiranja Savezne Republike Jugoslavije navodi da: "*Vojni zapovjednik mora uspostaviti učinkovit sustav prikupljanja obavještajnih podataka za prikupljanje i procjenu informacija o potencijalnim ciljevima. Zapovjednik također mora usmjeriti svoje snage na korištenje raspoloživih tehničkih sredstava za pravilno identificiranje ciljeva tijekom operacija.*" Dostupno na: https://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal (27.9.2023).
[173] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 114, str. 476.

informacije nepotpune, opseg napada možda će morati biti ograničen samo na one ciljeve o kojima postoji dovoljno informacija da se utvrdi može li se objekt smatrati vojnim ciljem.[174] Tallinnski priručnik 2.0 dodatno naglašava da napadač mora u svakom trenutku kontinuirano paziti da taj napad bude proporcionalan. Ako napadač postane svjestan da će napad koji se izvodi neočekivano rezultirati prekomjernom kolateralnom štetom, mora prekinuti napad.[175] Prilikom izvođenja takvih kibernetičkih operacija napadač bi trebao imati posebnu tehničku stručnost kako bi se analizirala ciljana mreža i sustavi s kojima je ona međusobno povezana.[176] Ako takva stručnost, nije dostupna, napadač će možda biti primoran suzdržati se od napada. U svakom slučaju, ako postoji mogućnost ozljede ili smrti civila, napadač unaprijed treba dati učinkovito upozorenje o kibernetičkim napadima koje namjerava izvesti.[177]

Kao što je ranije navedeno, kibernetički napadi ponekad mogu uzrokovati i manje štete civilima ili civilnoj infrastrukturi od kinetičkih napada.[178] Na primjer, kibernetički napad kojim bi bili oštećeni sustavi za upravljanje strojevima u tvornici izazvao bi daleko manje civilne žrtve nego da je ta ista tvornica bila bombardirana ili napadnuta nekim drugim kinetičkim sredstvom. Stoga bi pravilo poduzimanja mjera opreza, u nekim slučajevima moglo podrazumijevati uporabu kibernetičkih napada radije nego uporabu klasičnih kinetičkih sredstava.[179] Međutim, opseg obveze pribjegavanja sofisticiranijoj kibernetičkoj tehnologiji nije u potpunosti utvrđen jer još uvijek ne postoji međunarodni konsenzus koji bi nalagao zaraćenim strankama da moraju u svakom trenutku koristiti najpreciznije ili tehnološki najnaprednije oružje.[180]

5.3.2. Mjere opreza u odnosu na posljedice napada

Pravilo mjera opreza u odnosu na posljedice napada zahtijeva da će stranke u sukobu, "*u najvećoj mogućoj mjeri nastojati iz blizine vojnih ciljeva udaljiti civilno stanovništvo, građanske osobe i civilne objekte što su pod njihovom kontrolom*" i "*poduzimati druge potrebne mjere opreza za zaštitu civilnog stanovništva, građanskih osoba i civilnih objekata što su pod njihovom kontrolom od opasnosti koje su posljedica vojnih operacija*".[181] Ovdje je riječ o pasivnim mjerama opreza koje moraju poduzeti stranke u sukobu u očekivanju mogućeg

[174] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 115, str. 478.
[175] *Ibid.*, Rule 117, str. 481.
[176] *Ibid.* Commentary on Rule 115, str. 478.
[177] *Ibid.* Commentary on Rule 120, str. 484.
[178] Droege, *op. cit.* (bilj. 50), str. 574.
[179] Diamond, Eitan, *op. cit*. (bilj. 78), str. 80.
[180] Droege, *op. cit.* (bilj. 50), str. 574.
[181] Protokol I., *op. cit.* (bilj. 29), čl. 58.

kibernetičkog napada. Pojednostavljeno, zaraćene stranke moraju učiniti sve što je moguće kako bi razdvojili svoju vojnu i civilnu kibernetičku infrastrukturu ili poduzeli druge mjere za zaštitu civila i civilne kibernetičke infrastrukture od opasnosti koje proizlaze iz vojnih operacija. Kao što navodi Tallinnski priručnik 2.0, to može uključivati "*odvajanje vojne od civilne kibernetičke infrastrukture; odvajanje računalnih sustava o kojima ovisi kritična civilna infrastruktura od interneta; sigurnosno kopiranje važnih civilnih podataka negdje drugdje; digitalno snimanje važnih kulturnih ili duhovnih objekata kako bi se olakšala rekonstrukcija u slučaju njihovog uništenja tijekom oružanog sukoba; i korištenje antivirusnih mjera za zaštitu civilnih sustava koji bi mogli pretrpjeti štetu ili uništenje tijekom napada na vojnu kibernetičku infrastrukturu*".[182] Međutim, mogućnost poduzimanja takvih mjera nije uvijek realna. Protokol I. ograničava pasivne mjere opreza pojmom "*u najvećoj mogućoj mjeri*". Taj pojam ograničava poduzimanje onih mjera koje nisu praktično moguće. Možda nije uvijek izvedivo da stranke u sukobu odvoje potencijalne vojne ciljeve od civilnih objekata. Iako bi to odvajanje teoretski moglo biti izvedivo, bilo bi iznimno nepraktično i skupo. Države bi morale izgraditi vlastitu kibernetičku infrastrukturu za vojnu upotrebu i uspostaviti svoje vlastite vojne komunikacijske sustave. Najradikalnija primjena tog pravila zahtijevala bi od država da onemoguće civilima korištenje kibernetičke infrastrukture, kako bi ih na taj način zaštitila od mogućih kibernetičkih napada. No, kako navodi MOCK "*jasno je da mjere opreza ne bi trebale ići dalje od točke u kojoj bi život stanovništva postao težak ili čak nemoguć*".[183] Prema tome, kada se odvajanje ne može provesti, stranka u sukobu ostaje dužna poduzeti druge potrebne mjere opreza kako bi osigurala da će civilna kibernetička infrastruktura kao i životi samih civila biti zaštićeni što je više moguće od učinaka kibernetičkih napada.[184]

6. OSTALA PRAVILA MEĐUNARODNOG HUMANITARNOG PRAVA PRIMJENJIVA NA KIBERNETIČKE NAPADE

Osim glavnih pravila međunarodnog humanitarnog prava o vođenju neprijateljstava - pravila razlikovanja, proporcionalnosti i mjera opreza, postoje i dodatna pravila kojima je također cilj zaštiti civile od posljedica neprijateljstava. Tu prvenstveno spadaju pravila o zabrani suvišnog ozljeđivanja ili nepotrebne patnje. Također, zbog velikog potencijala kibernetičkih napada da se izvode prikriveno ili uz zavaravanje neprijatelja potrebno je utvrditi

[182] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 121, str. 486.
[183] Sandoz, Swinarski, Zimmerman, *op. cit*. (bilj. 98), paragraf 2245.
[184] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 121, str. 489.

kako se zabrana perfidije primjenjuju na te operacije. Valja svakako spomenuti i pravo neutralnosti, utemeljeno na običajnopravnim pravilima i Haškim konvencijama, koje zbog činjenica da se kibernetičko ratovanje provodi u kibernetičkom prostoru koji ne poznaje geografske granice te međusobne povezanosti kibernetičke infrastrukture može biti ugroženo.

6.1. ZABRANA SUVIŠNOG OZLJEĐIVANJA I NEPOTREBNE PATNJE

Navedeno pravilo zabranjuje uporabu oružja koje će uzrokovati nanošenje nepotrebne patnje. Međunarodni sud definirao je nepotrebnu patnju kao „*štetu veću od one koja je neizbježna kako bi se postigli legitimni vojni ciljevi*".[185] Također Međunarodni sud je zaključio kako "*države nemaju neograničenu slobodu u izboru sredstava oružja koje koriste*" te da je "*zabranjeno nanošenje nepotrebne patnje borcima: sukladno tome zabranjeno je koristiti oružje koje im nanosi takvu štetu ili beskorisno pogoršava njihovu patnju*".[186] Bitno je za naglasiti kako se ta zabrana odnosi isključivo na borce, članove organiziranih naoružanih skupina i civile koji izravno sudjeluju u neprijateljstvima.[187] Ostale osobe ne mogu biti meta napada, a moguću kolateralnu štetu prema takvim osobama uređuje pravilo proporcionalnosti.

Jednako kao i ostala pravila međunarodnog humanitarnog prava, i zabrana suvišnog ozljeđivanja i nepotrebne patnje je primjenjiva u kibernetičkom prostoru. Pa je tako zabranjeno koristiti sredstva ili metode kibernetičkog ratovanja koji su takve prirode da uzrokuju suvišne ozljede ili nepotrebnu patnju.[188] Zbog svoje specifične prirode, postoji puno manja opasnost da će kibernetička sredstva prekršiti navedenu zabranu. Ipak, mogući su i takvi scenariji. Pa bi tako kibernetički napad koji je uništio medicinsku dokumentaciju neprijateljskog vojnog zapovjednika mogao dovesti do toga da se vojnom zapovjedniku pruži neprikladan medicinski tretman koji uzrokuje nepotrebnu patnju.[189] U tom slučaju napadač bi prekršio zabranu suvišnog ozljeđivanja ili nepotrebne patnje. S obzirom na veliki broj čimbenika koji mogu utjecati na tu procjenu, činjenicu je li napadač prekršio pravilo zabrane suvišnog ozljeđivanja ili nepotrebne patnje najbolje je procjenjivati od slučaja do slučaja. U slučaju sumnje može se primijeniti pravilo prema kojemu je kibernetički napad nedopušten ukoliko su njegove posljedice slične kinetičkom napadu koji krši zabranu nepotrebne patnje.[190]

[185] ICJ, *op. cit*. (bilj. 33), paragraf 78.
[186] *Ibid.*
[187] MOCK, *op. cit*. (bilj. 61), str. 46.
[188] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Rule 104, str. 453.
[189] Gervais, *op. cit.* (bilj. 109), str. 41.
[190] *Ibid.*

6.2. PERFIDIJA

Protokol I. definira perfidiju kao „*čine kojima se zadobiva povjerenje protivnika kako bi ga se uvjerilo da ima pravo na zaštitu ili obvezu da pruži zaštitu na temelju pravila međunarodnog prava primjenjivih u oružanim sukobima, s namjerom da se to povjerenje iznevjeri*".[191] Sukladno tome, zabranjeno je ubiti, raniti ili zarobiti neprijatelja služeći se perfidijom. Na primjer, ukoliko se jedna strana pravi da je onesposobljena zbog ranjavanja ili bolesti, a zatim iskoristi protivnikovu dobru vjeru kako bi napala neprijateljskog borca to će predstavljati zabranjeno perfidno ponašanje.[192] Takav čin iskorištavanja zadobivenog povjerenja je nedopušten.

Već ranije spomenute specifične karakteristike kibernetičkog prostora i kibernetičkih sredstava pružaju mnoštvo mogućnosti i tehnika za korištenjem perfidnog ponašanja. Pa bi tako neki od primjera perfidnog ponašanja uključivali prikrivanje podrijetla kibernetičkih operacija lažiranjem internetskog protokola, manipuliranje podacima kako bi se pogrešno navelo neprijatelja da vjeruje kako se protivničke snage namjeravaju predati, ili slanje naizgled bezazlenih civilnih privitaka e-pošte pojedinačnim primateljima u vojnom stožeru, uzrokujući da oni nenamjerno zaraze računalne sustave zlonamjernim softverom.[193] Kako navodi Tallinnski priručnik 2.0 "*U vođenju neprijateljstava koja uključuju kibernetičke operacije, zabranjeno je ubiti ili ozlijediti protivnika pribjegavanjem perfidnosti.*".[194] Važno je za istaknuti to, da bi se prekršila zabrana perfidije, perfidni čin mora biti neposredan uzrok smrti ili ranjavanja.[195] Ukoliko je izvršeno perfidno ponašanje, ali do smrti ili ranjavanja je došlo zbog nekog drugog razloga tada zabrana nije prekršena.[196] U komentaru Protokola I. navodi se nasuprot tome da čak i "*pokušaj ili neuspješan čin perfidije također potpada pod opseg ove zabrane*".[197] S druge strane, kibernetičke operacije koje nanose samo fizičku ili funkcionalnu štetu kibernetičkoj infrastrukturi kao i drugi oblici onesposobljavanja takve infrastrukture, čak i ako se provode pomoću perfidije, ne bi potpadali pod zabranu perfidnog ponašanja.[198]

Prema članku 37. Protokola I „*hinjenje statusa civila ili neborca*" jedan je od primjera nedopuštenog perfidnog ponašanja.[199] Ukoliko bi napadači zavaravali svoje protivnike na način da oni pomisle kako kibernetički napad potječe od civila ili neborca tada bi oni kršili zabranu

[191] Protokol I., *op. cit.* (bilj. 29), čl. 36.
[192] MOCK, *op. cit*. (bilj. 61), str. 54.
[193] Melzer, *op. cit*. (bilj. 9), str. 32.
[194] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Rule 122, str. 490.
[195] *Ibid.*, Commentary on Rule 122, str. 492.
[196] *Ibid.*
[197] Sandoz, Swinarski, Zimmerman, *op. cit*. (bilj. 98), paragraf 1493.
[198] Melzer, op. cit. (bilj. 9), str. 32.
[199] Protokol I., *op. cit.* (bilj. 29), čl. 37(1).

perfidije. Ipak, s obzirom da se ova odredba odnosi samo na napade usmjerene prema protivnicima u oružanom sukobu, ostaje nejasno jesu li dopuštene perfidne radnje kojima se zavaravaju treće strane, odnosno nezaraćene države.[200] Takva je situacija postojala tijekom kibernetičkih napada u rusko-gruzijskom sukobu 2008. godine, kada su hakeri, pretvarajući se da su ti kibernetički napadi potekli iz Gruzije, napali servere međunarodnih banaka.[201] Kao odgovor na takav napad međunarodne banke su automatski gruzijskim bankama ograničile pristupa svojim serverima.[202] Međunarodno humanitarno pravo zabranjuje svaku kibernetičku operaciju koja bi se pretvarala da potječe iz nezaraćene države, ali s obzirom da Gruzija nije bila nezaraćena država takvo pravilo ovdje nije bilo primjenjivo. Ipak, iako međunarodno humanitarno pravo izričito ne zabranjuje takvo ponašanje, da su hakeri svoje napade usmjerili na državu koja je imala napetosti s Gruzijom, ova vrsta perfidnog ponašanja mogla je rezultirati negativnim posljedicama, pa čak i mogućim otvaranjem novog sukoba.[203]

Nadalje, kao jedan od zabranjenih oblika perfidije Protokol I. navodi i "*hinjenje zaštićenog statusa upotrebom znakova, obilježja ili odora Ujedinjenih naroda, neutralnih država ili drugih država koje nisu stranke sukoba*".[204] U kontekstu kibernetičkog prostora, postavlja se pitanje odnosi li se ta zabrana isključivo na upotrebu elektroničkih reprodukcija znakova i obilježja ili bi i slanje e-pošte preko lažirane domene neke treće države ili međunarodne organizacije, kao na primjer UN-a, predstavljalo perfidno ponašanje? Tallinnski priručnik 2.0 razlikuje dva pristupa. Prema prvom pristupu, zabranjene su samo kibernetičke operacije koje koriste elektroničke reprodukcije relevantnih znakova ili obilježja.[205] U tom slučaju, slanje e-pošte s lažirane domene UN-a ne bi predstavljalo zabranjeno perfidno ponašanje. Prema drugom pristupu, koji se temelji na tehnološkoj interpretaciji teksta, ukoliko bi slanje e-pošte preko lažirane domene zadobilo povjerenje protivnika u povezanost pošiljatelja s UN-om, tada bi takvo ponašanje bilo zabranjeno.[206]

Konačno, treba napraviti razliku između perfidije, koja je zabranjena, i dopuštenih ratnih varki. Ratne varke, odnosno *ruse de guerre,* definirane su kao "*čini kojih je svrha zavesti protivnika u bludnju ili navesti ga da se ponaša nesmotreno, ali kojima se ne krši nijedno*

[200] Gervais, *op. cit.* (bilj. 109), str. 41.
[201] Swanson, Lesley "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict", Loyola of Los Angeles International and Comparative Law Review, Vol. 303/2010, str. 320.
[202] Markoff, John, "Before the Gunfire, Cyberattacks", The New York Times, 2008), Dostupno na: http://www.nytimes.com/2008/08/13/technology/13cyber.html?ref=europe (27.9.2023).
[203] Gervais, *op. cit.* (bilj. 109), str. 41.
[204] Protokol I., *op. cit.* (bilj. 29), čl. 37(1).
[205] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 124, str. 497.
[206] *Ibid.*

pravilo međunarodnog prava primjenjivo u oružanim sukobima i koji nisu perfidni jer se njima ne zadobiva povjerenje protivnika glede zaštite na temelju toga prava".[207] Ratne varke smatraju se uobičajenom taktikom konvencionalnog ratovanja. Radnje kao što su iznenadni napadi, simuliranje napada ili povlačenja smatraju se dozvoljenim pokušajima da se utječe na neprijatelja i da se stekne vojna prednost.[208] Pa su tako, neposredno prije invazije na Irak 2003. godine, SAD upale u sustave iračkog Ministarstva obrane te poslale iračkim vojnim časnicima e-poštu u kojoj se navodi da je cilj SAD-a samo smijeniti Sadama Huseina s vlasti i da nema interesa da se naudi iračkim vojnim snagama.[209] Mnogi irački vojni časnici napustili su svoje položaje, čime je svrha ratne varke ispunjena.[210] Upravo takva uporaba kibernetičkih sredstava, koja ne krši međunarodno humanitarno pravo i koja poštuje zabranu perfidije nije zabranjena.

6.3. NEUTRALNOST

Iako su pravo neutralnosti i međunarodno humanitarno pravo dva različita pravna režima, međusobno su povezani jer neutralne države imaju ulogu u primjeni pravila međunarodnog humanitarnog prava. To je posebno vidljivo kod kibernetičkog ratovanja kada bi se zbog međusobne povezanosti kibernetičke infrastrukture pri provođenju kibernetičkih napada stranka u sukobu mogla koristiti privatnom ili javnom neutralnom kibernetičkom infrastrukturom. Zato je bitno pobliže pojasniti kako se ta pravila primjenjuju na kibernetičke napade. Pravila neutralnosti temelje se na V. i XIII. Haškoj konvenciji i međunarodnom običajnom pravu. Osim prava, Haške konvencije propisuju i obvezu neutralnih država da ne sudjeluju u sukobu kao i obvezu zaraćenih stranaka da poštuju nepovredivost neutralnih država. Pravilo neutralnosti dopušta državi da se proglasi neutralnom u sukobu i time se štiti od napada zaraćenih stranaka. Neutralne države ostaju zaštićene sve dok vojno ne sudjeluju ili ne doprinose zaraćenim državama ili dopuštaju da se njihov teritorij koristi u vojne svrhe.

Prema Međunarodnom sudu, neutralnost je temeljno načelo međunarodnog prava koje se primjenjuje "*bez obzira na vrstu oružja koje se može koristiti*".[211] Tallinnski priručnik 2.0 navodi da se pravila neutralnosti primjenjuju i na kibernetičke operacije.[212] Nepovredivost

[207] Protokol I., *op. cit.* (bilj. 29), čl. 37(2).
[208] Gervais, *op. cit.* (bilj. 109), str. 41.
[209] Clarke, Richard, A; Knake, Robert, K., Cyber war – Next treath to National Security and What To Do About It. HarperCollins e-books, str. 12., Dostupno na: https://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20%28Richard%20A%20Clarke%29%20%282010%29.pdf (27.9.2023).
[210] *Ibid.*, str. 12.
[211] ICJ, *op. cit*. (bilj. 33), paragraf 89.
[212] Tallinn Manual 2.0, *op. cit.* (bilj. 21), str. 553.

neutralnog teritorija propisana je člankom 1. V. Haške konvencije i člankom 1. XIII. Haške konvencije. Zaraćenim strankama je zabranjeno voditi neprijateljstva unutar neutralnog teritorija. No, moguća je situacija da kibernetički napad na vojni cilj na zaraćenom području ima učinke i na neutralnom teritoriju. Na primjer, napad na telekomunikacijske sustave zaraćene države može dovesti do smetnji u radu telekomunikacijskih sustava neutralne države. Tallinnski priručnik 2.0 navodi da, pod uvjetom da takvi učinci nisu predvidljivi, takav napad ne krši pravila neutralnosti.[213]

Jednako kao što je zabranjeno zaraćenim strankama da provode kibernetičke napade unutar neutralnog teritorija isto tako neutralna država ne smije dopustiti zaraćenim strankama da premještaju trupe, ratno streljivo ili zalihe kroz neutralni teritorij.[214] Ako neutralna država dopusti da se njezin teritorij koristi u te svrhe, tada je pravila neutralnosti više ne štite. Tallinnski priručnik 2.0 navodi da se ta odredba V. Haške konvencije prvenstveno odnosi na fizički transport kibernetičkog oružja.[215] No, postavlja se pitanje što je sa situacijom kada se kibernetičko oružje prenosi putem neutralne kibernetičke infrastrukture? Zbog složenosti kibernetičke infrastrukture i činjenice da će informacije do svog odredišta ići najkraćim mogućim putem, obveza neutralne države da spriječi kibernetički napad koji potječe s njenog teritorija bila bi nerealna.[216] Ipak, većina međunarodne skupine stručnjaka smatra kako je prijenos kibernetičkog oružja preko kibernetičke infrastrukture koja se nalazi u neutralnoj državi također zabranjen na temelju tog članka.[217] Ukoliko zlonamjerni softver ili DoS napad prolazi kroz neutralnu kibernetičku infrastrukturu, neutralna država mora učiniti sve u njenoj moći kako bi spriječila takav prijenos, ali samo ako zna za njega i može poduzeti mjere da ga prekine.[218]

V. Haška konvencija dalje predviđa da neutralne države ne trebaju "*zabraniti ili ograničiti uporabu u ime zaraćenih stranaka telegrafa ili telefonskih kabela ili bežičnih telegrafskih uređaja koji pripadaju njemu ili tvrtkama ili privatnim osobama*".[219] Ta mogućnost postoji samo ako neutralne države dopuštaju upotrebu svoje telekomunikacijske infrastrukture nepristrano, odnosno ako upotrebu dopuštaju svim zaraćenim strankama. Iako su postojala neslaganja odnosi li se taj članak i na kibernetičku infrastrukturu, prema

[213] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 150, str. 554.
[214] Hague Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 1907, International Humanitarian Law Databases, čl. 8. Dostupno na: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-v-1907?activeTab=default (28.9.2023).
[215] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 151, str. 557
[216] Gervais, *op. cit.* (bilj. 109), str. 41.
[217] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 151, str. 555.
[218] *Ibid.*
[219] V Haška konvencija, *op. cit*. (bilj. 214), čl. 8.

Tallinskom priručniku 2.0 taj se članak može primijeniti i na kibernetičke komunikacijske sustave.[220]

Također, V. Haška konvencija izričito zabranjuje da zaraćene stranke: (a) podignu na teritoriju neutralne Sile bežičnu telegrafsku stanicu ili druge uređaje u svrhu komunikacije sa zaraćenim snagama na kopnu ili moru; te (b) koriste bilo koje postrojenje ove vrste koje su uspostavili prije rata na teritoriju neutralne Sile u čisto vojne svrhe, a koje nije bilo otvoreno za služenje javnim porukama.[221] U kontekstu kibernetičkih operacija, to bi značilo da neutralna država ne smije dopustiti stranci u sukobu da koristi svoju već postojeću kibernetičku infrastrukturu na neutralnom teritoriju u vojne svrhe ili da uspostavi bilo kakvu novu kibernetičku infrastrukturu u te svrhe.[222]

Konačno, ukoliko neutralna država ne uspije prekinuti zaraćenu stranku u kršenju neutralnosti na svojem teritoriju, oštećena država tada može poduzeti potrebne mjere kako bi takvo kršenje zaustavila. Te mjere uključuju i potencijalne kibernetičke operacije protiv neutralne države. Ipak, potrebna su određena ograničenja. Prvenstveno, oštećena država mora obavijestiti neutralnu državu o kršenju neutralnosti i dati joj razumno vrijeme da to kršenje prekine.[223] Mjere će se moći primijeniti samo ako neutralna država ne želi ili nije u stanju ispuniti svoje obveze prema oštećenoj državi.[224] Drugo, povreda teritorija neutralne države mora biti ozbiljna, odnosno stranka koja krši neutralni status mora tim kršenjem steći značajnu vojnu prednost nad protivnikom.[225] I treće, oštećenoj državi dopušteno je poduzeti mjere protiv neutralne samo ako to kršenje predstavlja ozbiljnu i neposrednu prijetnju njezinoj sigurnosti i samo ako ne postoji druga alternativa.[226]

7. KIBERNETIČKI NAPADI – BUDUĆA METODA RATOVANJA

Kibernetički napadi i kibernetičko ratovanje predstavljaju relativno novu prijetnju. Za očekivati je kako će se uporaba kibernetičkih sredstava ratovanja u narednim godinama sve više povećavati te kako će se države sve više upuštati u razorne kibernetičke sukobe. S daljnjim razvojem tehnologije i nastavkom umrežavanja svijeta opasnost za civilnu populaciju bit će sve veća. Iako se, u svrhu zaštite civila i civilnih objekata, pravila međunarodnog humanitarnog

[220] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 151, str. 555.
[221] V Haška konvencija, *op. cit*. (bilj. 214), čl. 3.
[222] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 152, str. 557-558.
[223] Droege, *op. cit.* (bilj. 50), str. 565-566.
[224] Tallinn Manual 2.0, *op. cit.* (bilj. 21), Commentary on Rule 153, str. 559.
[225] *Ibid.*
[226] Droege, *op. cit.* (bilj. 50), str. 565-566.

prava tumačenjem mogu primijeniti i na kibernetičke napade, trenutno stanje međunarodnog humanitarnog prava koje regulira kibernetičke operacije nije u potpunosti zadovoljavajuće.[227]

Postoje različiti prijedlozi kako pristupiti tome problemu. Jedan od njih je usvajanje pravila o digitalnim sigurnim utočištima, to jest civilnim objektima gdje će biti zabranjeno provoditi kibernetičke operacije, po uzoru na demilitarizirane zone iz članka 60. Protokola I.[228] Primjenom tog pravila, određeni dijelovi kibernetičke infrastrukture, i to oni koji se najviše koriste u civilne svrhe, bili bi izuzeti od napada. Na to se nadovezuje i prijedlog proširenje popisa "*postrojenja i instalacija koje sadrže opasne sile"* iz članka 56. Protokola I.[229] Tada se glavne internetske točke za razmjenu ili središnji serveri na koje se oslanjaju milijuni važnih civilnih funkcija, zbog činjenice da opasnosti za civilno stanovništvo nadmašuju vojnu prednost napada na njih, ne bi mogli napadati čak i u slučaju kad bi se klasificirali kao vojni ciljevi.[230] Postoje i razmišljanja da se neka sredstva i metode kibernetičkog ratovanja u potpunosti zabrane ili reguliraju međunarodnim ugovorom.[231] To bi se moglo učiniti uspostavljanjem međunarodne organizacije za kibernetičku sigurnost, po uzoru na Međunarodnu agenciju za atomsku energiju, kao neovisne platforme za međunarodnu suradnju u polju kibernetički operacija.[232]

Jedan sveobuhvatni međunarodni ugovor koji regulira kibernetičko ratovanje ipak bi bio najkorisniji dodatak međunarodnom humanitarnom pravu. Takav međunarodni ugovor, definirao bi trenutno sporne pojmove *napada*, *objekata dvojne namjene* i *podataka*, te bi, imajući u vidu opseg međunarodnog humanitarnog prava koji po samoj svojoj prirodi mora uzeti u obzir vojne potrebe i realnost rata, pobliže razjasnio primjenu pravila tog pravnog režima na kibernetičko ratovanje. Tom razjašnjavanju će svakako pomoći i Tallinnski priručnik 3.0, koji je trenutno u procesu izrade.[233]

Međutim, u trenutnoj međunarodnoj klimi, izrada takvog međunarodnog ugovora malo je vjerojatna.[234] Iako se svijest o potrebi takvog dokumenta u zadnje vrijeme povećala, nije realno za očekivati da će do njegovog usvajanja doći u bliže vrijeme. Realnije je za očekivati da će veliki broj pravila nastati iz prakse i običaja koje će države razvijati u provođenju

[227] Schmitt, *op. cit.* (bilj. 101), str. 353.
[228] Segal, Adam, "Cyber space governance: the next step'", Council on Foreign Relations, Policy Innovation Memorandum, 2011, str. 3.
[229] Geiss; Lahmann, op.cit. (bilj. 82), str 11.
[230] Droege, *op. cit.* (bilj. 50), str. 577.
[231] *Ibid.*
[232] Segal, *op. cit.* (bilj. 229) str. 3.
[233] *v. više.* News, CCDCOE, Dostupno na: https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/ (27.10.2023).
[234] Gervais, *op. cit.* (bilj. 109), str. 45.

kibernetičkih operacija, što će možda u konačnici rezultirati dovoljno širokim konsenzusom kako bi se moglo pristupiti izradi međunarodnog ugovora.

8. ZAKLJUČAK

Od kibernetičkih napada na Estoniju 2007. godine, preko Stuxneta, pa do trenutnog rata u Ukrajini, kibernetički napadi postali su široko rasprostranjena metoda ratovanja. Ipak, unatoč brojnim kibernetičkim napadima, stvarno iskustvo država s kibernetičkim ratovanjem je ograničeno, te je do danas iskorišten samo mali potencijal koji takvi napadi imaju. Za očekivati je kako će se broj kibernetičkih napada i njihovo korištenje u budućim sukobima među državama bitno povećavati.

Unatoč protivljenju nekih država, danas je općeprihvaćeno kako su odredbe međunarodnog humanitarnog prava dovoljno široke kako bi se odnosile i na kibernetičke napade. Takav isti stav zauzimaju i MOCK, NATO, kao i međunarodna skupina stručnjaka koja je sastavljala Tallinnski priručnik 2.0. Dakako, kako bi pravila međunarodnog humanitarnog prava mogla biti primjenjiva mora biti riječ o onim kibernetičkim operacijama koje se provode u kontekstu oružanog sukoba i koje potpadaju pod pojam napada kako je definiran u međunarodnom humanitarnom pravu.

Međutim, iako nema sumnje da se međunarodno humanitarno pravo primjenjuje na kibernetičke napade, još uvijek postoje nedoumice kako ga točno treba primjenjivati. Činjenice da se kibernetički napadi ne provode uporabom kinetičke sile, da se provode u kibernetičkom prostoru gdje istovremeno djeluje velik broj ljudi te da kibernetička infrastruktura ima i civilnu i vojnu namjenu, mogu dovesti do poteškoća u primjeni tradicionalnih pravila međunarodnog humanitarnog prava o vođenju neprijateljstava. Primjena pravila razlikovanja, proporcionalnosti i mjera opreza otežana je zbog činjenice da se definicije i terminologija tog pravnog režima temelje na osnovi osmišljenoj za tradicionalno kinetičko ratovanje. Specifičnosti kibernetičkih napada također uzrokuju poteškoće i kod primjena pravila zabrane suvišnog ozljeđivanja i nepotrebne patnje kao i kod zabrane perfidije. Niti pravo neutralnosti, zbog međusobne povezanosti kibernetičkih mreža i sustava, nije izuzeto od utjecaja kibernetičkih napada. Preslikati nove realnosti kibernetičkog ratovanja na ta tradicionalna pravila o vođenju neprijateljstava nije jednostavno, a u nekim slučajevima nije niti moguće. Nejasnoće i složenosti, koje proizlaze iz primjene pravila međunarodnog humanitarnog prava, otvaraju mogućnost pojedinim državama da širokim tumačenje tih odredaba nastave provoditi kibernetičke napade ne uzimajući u obzir zaštitu i ograničenja tog režima. Zbog toga je

potrebno što prije redefinirati sporne pojmove poput *napada*, *objekata dvojne namjene* i *podataka* ali uzimajući u obzir kontekst kibernetičkih napada i kibernetičkog prostora u kojem se ti napadi provode.

Daljnjim razvojem i napretkom tehnologije, kao i nastavkom umrežavanja svijeta, kibernetički napadi bit će sve učestaliji, a njihove moguće posljedice sve smrtonosnije. Zbog toga je iznimno važno što prije dati odgovor na navedena pitanja kako bi se civilima i civilnim objektima mogla pružiti učinkovita zaštita od štetnih učinaka kibernetičkog ratovanja. Do tada, ukoliko zaraćene stranke tijekom oružanog sukoba odaberu kibernetičke napade kao sredstvo i metodu ratovanja, moraju uzeti u obzir postojeći pravni režim kao minimalni skup pravila koja, unatoč njihovim ograničenjima, treba poštivati.

LITERATURA

Knjige:

1. Andrassy, Juraj; Bakotić, Božidar; Seršić, Maja; Vukas, Budislav, Međunarodno pravo - 3. dio, Školska knjiga, Zagreb, 2006;
2. Clarke, Richard, A; Knake, Robert, K., Cyber war – Next treath to National Security and What To Do About It, HarperCollins e-books, Dostupno na: https://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20%28Richard%20A%20Clarke%29%20%282010%29.pdf (27.9.2023);
3. Dinstein, Yoram, "The Conduct of Hostilities under the Law of International Armed Conflict", Cambridge University, 2004;
4. Sandoz, Yves; Swinarski, Christophe; Zimmerman, Bruno (ur.), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ICRC, Geneva, 1987 (ICRC Commentary on the APs).

Članci:

1. Antolin- Jenkins, Vida, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?", Naval Law Review. Vol.132/2008;
2. Baenzer, Marie; Robin, Patrice, "Stuxnet", Center for Security Studies, ETH Zurich, 2018, Dostupno na: https://www.researchgate.net/publication/323199431_Stuxnet;
3. Blount, Roy, Making Sense of Robert E. Lee, Smithsonian Magazine, 2003, Dostupno na: https://www.smithsonianmag.com/history/making-sense-of-robert-e-lee-85017563/ (26.9.2023);
4. Diamond, Eitan, "Applying International Humanitarian Law to Cyber Warfare", Institute for National Security Studies, 2014;
5. Dinniss, Harrison, Heather, A., "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", Israel Law Review, Vol. 48/2015
6. Dormann, Kunt; Gisel, Laurent; Rodenhauser, Tilman, "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts", International Review of the Red Cross, Vol. 102/2020;

7. Droege, Cordula, “Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians”, International Review of the Red Cross, Vol. 94/2012;
8. Fenton, Hensey, A., III, “Proportionality and its applicability in the realm of cyber-attacks“, Duke Journal of Comperative & International Law, Vol. 29/2019;
9. Geiss, Robin; Lahmann, Henning, “Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space“ Israel Law Review, Vol. 45/2012;
10. Gervais, Michael, “Cyber Attacks and the Laws of War“, Journal of War & Cyber Warfare, Vol. 1/2012;
11. Graham, D. E., “Cyber Threats and the Law of War“, Journal od National Security and Policy, Vol. 4/2010;
12. Green, Leslie, C., “The Law of War in Historical Perspective”, International Law Studies, Vol. 72/1998;
13. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J., “The Law of Cyber-Attack”, California Law Review, Vol.100/2012;
14. Hongsheng, Sheng, “The Evolution of the Law of War”, Chinese Journal of International Politics, Vol 1/2006;
15. Jensen, Eric, T., “Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?“, American University International Law review, Vol.18/2003 Dostupno na: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1208&context=auilr (27.9.2023);
16. Jensen, Eric, T., „Cyber Attacks: Proportionality and Precautions in Attack“, International Law Studies, Vol. 98/2013;
17. Lin, Herbert, “Cyber conflict and international humanitarian law”, International Review of the Red Cross, Vol 94/2012;
18. Mačák, Kubo, “Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law”, Israel Law Review, Vol. 58/2015
19. Mayuko, Torii, „“Issues concerning Cyber Attacks in Light of the Law of Armed Conflict“, Air and Space Power Studies, Vol. 7. Dostupno na https://www.mod.go.jp/asdf/meguro/center/Eimg/10aspw7.pdf (27.9.2023);
20. Melzer, Niels, Interpretative guidance on the notion of Direct participation in hostilities under international humanitarian law, ICRC, 2009;

21. Melzer, Nils, “Cyberwarfare and International Law”, UNIDR Resources, 2011, Dostupno na: https://unidir.org/sites/default/files/publication/pdfs//cyberwarfare-and-international-law-382.pdf (26.10.2023);
22. Pascucci, Peter, “Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution”, Minnesota Journal of International Law, 215/2017;
23. Schmidt, Andreas, “The Estonian Cyberattacks”, 2013, Dostupno na: https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks (26.9.2023);
24. Schmitt, Michael, N., „Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics“, Harvard National Security Journal, 2013;
25. Schmitt, Michael, N., “Cyber operations and the jus in bello: key issues“, International Law Studies, Vol. 87/2011;
26. Schmitt, Michael, N., “The Law of Cyber Warfare: Quo vadis?”, Stanford Law and Policy Review, Vol. 25/2014;
27. Schmitt, Michael, N., “Wired warfare 3.0: Protecting the civilian population during cyber operations“, International Review of the Red Cross, Vol. 101/2019;
28. Schmitt, Michael, N.; O’Donnel, Brian T., “Computer Network Attack and International Law“, International Law Studies, Vol. 76/2002;
29. Schmitt, Michael; Vihul, Liis, "International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms" Just Security, 2017, Dostupno na: https://www.justsecurity.org/42768/international-cyber-law- (26.9.2023);
30. Segal, Adam, “Cyber space governance: the next step’“, Council on Foreign Relations, Policy Innovation Memorandum, 2011;
31. Sohail, Humna, “Fault Lines In The Application Of International Humanitarian Law To Cyberwarfare“, Journal of Digital Forensics, Security and Law, Vol.17/2022;
32. Swanson, Lesley “The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict“, Loyola of Los Angeles International and Comparative Law Review, Vol. 303/2010.

Međunarodni ugovori:

1. Bečka konvencija o pravu međunarodnih ugovora, 1969, Narodne novine, Međunarodni ugovori, 13/1993;
2. Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight (Petrogradska deklaracija), 1868, Inetrantional Humanitarian Law

Databases, Dostupno na: https://ihl-databases.icrc.org/en/ihl-treaties/st-petersburg-decl-1868 (28.9.2023);
3. Deklaracija o zabrani upotrebe metaka koji se u tijelu lako raširе ili spljošte, 1899, Dostupno na: https://avalon.law.yale.edu/19th_century/dec99-03.asp (28.9.2023);
4. Dopunski protokol Ženevskim konvencijama od 12. kolovoza 1949. o zaštiti žrtava međunarodnih oružanih sukoba (Protokol I), Narodne novine, Međunarodni ugovori, 5/1994;
5. Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 1907, International Humanitarian Law Database, Dostupno na https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907 (26.9.2023);
6. Hague Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 1907, International Humanitarian Law Databases, Dostupno na: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-v-1907?activeTab=default (28.9.2023);
7. Hague Convention (VIII) relative to the Laying of Automatic Submarine Contact Mines, 1907, International Humanitarian Law Databases, Dostupno na: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-viii-1907 (28.9.2023);
8. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, (Protocol I), 1977, International Humanitarian Law Database, Dostupno na https://ihldatabases.icrc.org/en/ihl-treaties/api-1977 (26.9.2023);
9. Rimski statut Međunarodnog kaznenog suda, Narodne novine, Međunarodni ugovori, 5/2001;
10. Ženevska konvencija o postupanju s ratnim zarobljenicima, 1949, NN 5/1994;
11. Ženevska konvencija o zaštiti građanskih osoba u vrijeme rata, 1949, NN 5/1994;
12. Ženevska konvencije za poboljšanje položaja ranjenika i bolesnika u oružanim snagama u ratu, 1949, NN 5/1994;
13. Ženevska konvencije za poboljšanje položaja ranjenika, bolesnika i brodolomaca oružanih snaga na moru, 1949, NN 5/1994.

Sudske odluke:

1. Final Report to the Prosecutor by the committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, 2003. Dostupno na:

https://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal (27.9.2023);
2. ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, Dostupno na: https://www.icj-cij.org/sites/default/files/case-related/95/095-19960708-ADV-01-00-EN.pdf (26.9.2023);
3. ICTY, Prosecutor v. Stanislav Galić, Trial Chamber judgment, 2003, Dostupno na https://www.icty.org/x/cases/galic/tjug/en/ (27.9.2023).

Dokumenti:

1. International Committee of the Red Cross, International humanitarian law and the challenges of contemporary armed conflicts - Report, 32nd International Conference of the Red Cross and the Red Crescent, 2015;
2. Schmitt, Michael (ur.), Tallinn Manual 2.0 on the International law Applicable to Cyber Operations, Cambridge University Press, 2017;
3. Second 'Pre-Draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security, 2020, Dostupno na https://ict4peace.org/wp-content/uploads/2020/12/200527-oewg-ict-revised-pre-draft.pdf (26.9.2023);
4. The General Orders No. 100: Instructions for the Government of the Armies of the United States in the Field (Lieber Code), International Humanitarian Law Database, Dostupno na https://ihl-databases.icrc.org/en/ihl-treaties/liebercode-1863 (26.9.2023)
5. United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 68th Session, UN Document A/68/98, 2013;
6. United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 70th Session, UN Document A/70/174.

Novinski članci:

1. Cieslak, Mark; Gerken, Tom, Ukraine crisis: Google Maps live traffic data turned off in country, BBC News, 2022, Dostupno na: https://www.bbc.com/news/technology-60561089 (26.9.2023);

2. Culliford, Elizabeth, Goodle temporarily disables Google Maps live traffic data in Ukraine, Reuters, 2022, Dostupno na: https://www.reuters.com/technology/google-temporarily-disables-google-maps-live-traffic-data-ukraine-2022-02-28/ (26.9.2023);
3. Markoff, John, "Before the Gunfire, Cyberattacks", The New York Times, 2008, Dostupno na: http://www.nytimes.com/2008/08/13/technology/13cyber.html?ref=europe (27.9.2023);
4. Ranger, Steve, Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar, Techrepublic, 2014, Dostupno na: http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/ (26.9.2023).

Ostali izvori:

1. CARNet CERT, DDoS napad, Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-09-240.pdf (27.10.2023);
2. CCDCOE, https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/ (27.10.2023);
3. Datreportal, https://datareportal.com/global-digital-overview (26.9.2023)
4. Hrvatska enciklopedija, mrežno izdanje, Leksikografski zavod Miroslav Krleža, 2021, Dostupno na: https://www.enciklopedija.hr/natuknica.aspx?id=68098 (26.10.2023);
5. MOCK, Customory IHL - Rules, Dostupno na: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule10#Fn_A84730F9_00002 (26.9.2023);
6. MOCK, Introduction to the Law of Armed Conflict, 2002, Dostupno na: https://www.icrc.org/en/doc/assets/files/other/law1_final.pdf__ghfg (27.9.2023);
7. MOCK, Međunarodno humanitarno pravo – odgovori na vaša pitanja, 2012, Dostupno na: https://www.hck.hr/UserDocsImages/publikacije/0703_002_IHL-answers_Couv_LR.pdf (26.9.2023);
8. U.S. Department of Defense – Contracts, Dostupno na: https://www.defense.gov/News/Contracts/ (26.9.2023).