

Aplikácia medzinárodného práva v kybernetickom priestore

V a l u c h, J.*

VALUCH, J.: Aplikácia medzinárodného práva v kybernetickom priestore. Právny obzor, 102, 2019, č. 2, s. 114 – 130.

The Application of International Law in Cyberspace. The development of science and technology entails a number of relevant legal issues which, apart from the entities concerned, also the scholars of jurisprudence intend to clarify. A typical example is the relation between cyberspace and international law. Unlike the national law, the situation is more complicated in the case of international law given the fact that states, being the traditional subjects of this field of law, are often motivated more by their own interests rather than the effort to actually solve the problems. The submitted paper analyses the possibilities for the application of international law in this field and the issues related thereto.

Key words: international law, cyberspace, state

Úvod

Dnes sa v porovnaní s minulosťou nachádzame v období, keď informačné technológie prenikajú takmer do všetkých oblastí života, čím sa informácie stávajú dostupnejšími, komunikácia flexibilnejšou a spoločnosť celkovo „rýchlejšou“. Na druhej strane sa však komunikácia a celkovo spoločnosť stáva väčšmi anonymnou a zraniteľnou.

Práve pomerne jednoduchá dostupnosť, ale i anonymita a priestorová neuchopiteľnosť informačných technológií spôsobujú, že sa čoraz väčšia časť aktivít presúva do kybernetického priestoru, umožňujúceho rýchle a jednoduché splnenie aj nekalých cieľov s minimálnym rizikom postihu. Kybernetický priestor sa tak v mnohých ohľadoch odlišuje od doposiaľ známych a využívaných úrovní priestoru. Azda najjednoduchšie a najvýstižnejšie ho charakterizuje to, že funguje vo virtuálnej rovine, ktorú nedokážeme vidieť ani uchopiť a môže v ňom byť aktívnych množstvo rozličných aktérov.¹

Celkovo možno povedať, že siete, zariadenia a služby informačných a komunikačných technológií sú čoraz dôležitejšie pre každodenný život. V roku 2016 takmer polovica sveta používala internet (3,5 miliardy užívateľov) a podľa niektorých odhadov bude do roku 2020 pripojených na internet viac ako 12 miliárd zariadení.² Novšie štatistiky uvádzajú, že k júnu 2018 bolo na celom svete viac ako 4,2 miliardy užívateľov internetu a ich počet neustále rastie.

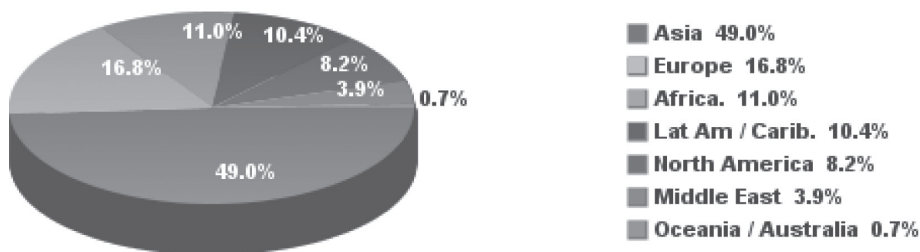
* JUDr. Jozef V a l u c h, PhD., Katedra medzinárodného práva a medzinárodných vzťahov, Právnická fakulta, Univerzita Komenského v Bratislave.

¹ Bližšie k vymedzeniu kybernetického priestoru pozri MELKOVÁ, M., SOKOL, T.: Kybernetický priestor ako nová dimenzia národnej bezpečnosti. In Bezpečnostné fórum 2015. I. zväzok. Banská Bystrica : Vydavateľstvo Univerzity Mateja Bela - Belianum, 2015, s. 55-56.

² *Global Cybersecurity Index 2017*, Geneva: International Telecommunication Union, 2017, s. 1; materiál dostupný na: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf, (navštívené dňa 09. 01. 2019).

S rastúcim počtom užívateľov ide ruka v ruke aj rastúci počet aktérov v kybernetickom priestore s rozdielnymi záujmami a cieľmi. Samozrejme, rozloženie aktérov v tomto type priestoru sa v rámci jednotlivých krajín či regiónov líši. V tabuľkách sú uvedení užívatelia podľa jednotlivých regiónov.

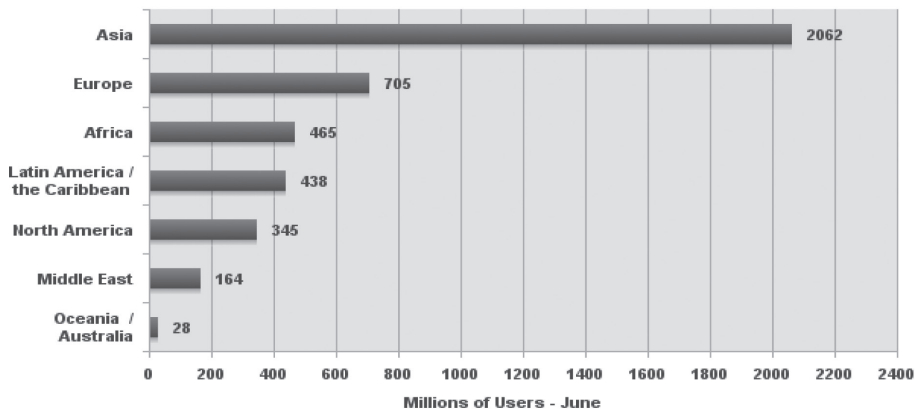
Užívatelia internetu vo svete podľa jednotlivých regiónov
k 30. júnu 2018, vyjadrení v percentách:



Basis: 4,208,571,287 Internet users in June 30, 2018

Zdroj: Internet World Stats³

Užívatelia internetu vo svete podľa jednotlivých regiónov
k 30. júnu 2018, vyjadrení v miliónoch:



Basis: 4,208,571,287 Internet users estimated in June 30, 2018

Zdroj: Internet World Stats⁴

³ Internet World Stats, dostupné na: <https://www.internetworldstats.com/stats.htm>.

⁴ Tamtiež.

Práve zväčšujúca sa základňa aktérov v tomto type priestoru a čoraz väčšia prepojenosť s každodennými aktivitami zdôrazňujú význam a aktuálnosť tejto problematiky.

Pokiaľ ide o bezpečnosť, množia sa názory, že zaručiť absolútnu bezpečnosť v tomto priestore nie je vzhľadom na jeho špecifiká možné. Ide o úroveň priestoru poskytujúcu okrem množstva výhod aj priestor na kybernetické hrozby a informačnú kriminalitu, ktoré zahŕňajú širokú škálu negatívnych fenoménov rôzneho stupňa závažnosti. V zmysle uvedeného vymedzenia sa na ďalších stranách pokúsime priblížiť vzt'ah kybernetického priestoru so všetkými jeho špecifikami a medzinárodného práva verejného ako súboru noriem upravujúcich vzťahy medzi subjektmi tohto právneho odvetvia, predovšetkým však štátmi.

Vymedzenie kybernetického priestoru a medzinárodného práva

Pre lepšie poňatie problematiky a súvisiacich pojmov sa pokúsime aspoň v stručnosti priblížiť základné pojmy. Medzinárodní právnici, resp. ich poňatie kybernetického priestoru je totiž ovplyvnené ich vnímaním toho, ako sú jednotlivé priestory poňaté medzinárodným právom.⁵

Pojem „kybernetický priestor“ použil po prvýkrát W. F. Gibson v krátkej poviedke *Burning Chrome* v roku 1982 a následne vo svojej sci-fi novele *Neuromancer* v roku 1984.⁶ Odvtedy rástla celosvetová popularita tohto pojmu v súvislosti s rýchlym a nezaostaviteľným využívaním kybernetického priestoru vo svete. Kybernetický priestor tak vytvoril špecifickú komunikačnú sieť s osobitým statusom, nepodriadenú v celosti konkrétnej krajine, právu alebo jurisdikcii. V dnešnom novodobom svete tak už nie je pravdou tvrdenie nemeckého filozofa K. Jaspersa, v ktorého zmysle nik nemôže žiadať, aby ho bolo na verejnosti počuť a súčasne aby ostal nepozorovaný.⁷ Internet je totiž pavučina sietí (prepojených sietí)⁸, v ktorej rámci môže mať elektronická komunikácia presne túto formu a v ktorej rámci bude niekto vypočutý a zároveň zostane nespozorovaný. Toto je to, čo je považované za skutočný „kybernetický priestor“.⁹

Inými autormi je kybernetický priestor definovaný napr. ako globálne, vzájomne prepojená sieť digitálnych informačných a komunikačných infraštruktúr vrátane internetu, telekomunikačných sietí, počítačových sietí a informácií v nich obsiahnutých.¹⁰ V našom článku budeme vychádzať predovšetkým z vymedzenia tohto typu priestoru, ktoré sa uvádza v dokumente Tallinn Manual 2.0. Ide o dokument vytvorený medzinárodnou

⁵ Bližšie pozri: TSAGOURIAS, N. The legal status of cyberspace. In Research Handbook on International Law and Cyberspace, s. 15, dostupné na: <http://www.e-elgar.com/shop/eeep/preview/book/isbn/9781782547396/> (navštívené dňa 19. 09. 2016).

⁶ KNORR, A. The Stability of Cyberspace. In POLČÁK, R., ŠKOP, M., ŠMAHEL, D. (Ed.) Cyberspace 2005. Brno : Masarykova Univerzita, 2006, s. 194, cit. podľa: GÁBRIŠ, T. *Cyber Law*. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2014, s. 14.

⁷ JASPERS, K. (Elexová, P. preklad): *Malá škola filozofického myslenia*. Bratislava : Kalligram, 2003, s. 108.

⁸ *Interconnected networks* = internet.

⁹ GÁBRIŠ, T. *Cyber Law* ... cit. dielo, s. 14-15.

¹⁰ MELZER, N. *Cyber Warfare and International Law*. UNIDIR Resources, 2011, s. 4.

expertnou skupinou, ktorá bola prizvaná Centrom výnimočnosti pre oblasť spoločnej kybernetickej obrany spolupracujúcim s NATO.

V zmysle tohto dokumentu pozostáva kybernetický priestor z fyzickej, logickej a sociálnej vrstvy. Fyzická vrstva zahŕňa fyzické sieťové komponenty, t. j. hardvér a inú infraštruktúru, ako sú káble, routre, servery a počítače. Logická vrstva pozostáva z prepojení, ktoré existujú medzi sieťovými zariadeniami. Obsahuje aplikácie, dáta a protokoly, ktoré umožňujú výmenu údajov naprieč fyzickou vrstvou. Sociálna vrstva zahŕňa jednotlivcov a skupiny zapojené do kybernetickej činnosti.¹¹

Pri poňatí kybernetického priestoru medzinárodným právom musíme vychádzať aj z osobitého charakteru medzinárodného práva. Pod týmto pojmom rozumieme medzinárodné právo verejné, ktoré možno definovať aj ako štandard správania, v danom momente pre štáty a ďalšie entity, ktoré mu podliehajú.¹²

Napriek tomu, že neexistuje žiadna norma, ktorá by obsahovala záväznú definíciu medzinárodného práva, na účely tejto práce je vhodné priblížiť aspoň základné charakteristické črty tohto právneho odvetvia. Nedostatok v podobe záväznej definície sa totiž snaží odstrániť veda medzinárodného práva v podobe viac či menej podrobných definícií medzinárodného práva verejného, ktoré však nemajú právnu záväznosť.

Jedna z najjednoduchších definícií medzinárodného práva verejného uvádza, že ide o súbor právnych noriem, ktoré upravujú vzťahy medzi štátmi a inými subjektmi medzinárodného práva.¹³ Pokiaľ ide o predmet medzinárodného práva, ani v tomto prípade záväzná obsahová definícia neexistuje. Možno však povedať, že z predmetu úpravy medzinárodného práva je vyčlenená matéria, ktorá je v obsahovom rozpore s jeho kogentnými normami. Ak by sa napr. aj takéto otázky stali predmetom zmluvnej úpravy, v zmysle článku 53 Viedenského dohovoru o zmluvnom práve je potrebné považovať túto úpravu za absolútne neplatnú.¹⁴ Na rozdiel od vnútroštátneho práva sú potom predmetom úpravy medzinárodného práva právne vzťahy vznikajúce, meniace sa alebo zánikajúce mimo rámca individuálneho štátu, t. j. v rámci procesu spolupráce, súperenia či nepriateľstva jednotlivých štátov, resp. subjektov pôsobiacich na medzinárodnej scéne.¹⁵ Predmetom úpravy tak môžu byť predovšetkým politické, ale aj iné špecifické vzťahy (obchodné, kultúrne a pod.) medzi jednotlivými subjektmi medzinárodného práva, ktoré sú upravené normami tohto právneho odvetvia. Z uvedeného vyplýva aj funkcia medzinárodného práva, ktorou nie je len koordinovať správanie štátov, ale prostredníctvom

¹¹ SCHMITT, M. N. (General Ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge : Cambridge University Press, 2017 (ďalej aj *Tallinn Manual 2.0*), s. 12.

¹² GRANT, J. P. – BARKER, J. C. *Parry & Grant Encyclopaedic Dictionary of International Law, Third Edition*. Oxford : Oxford University Press: 2009, s. 30.

¹³ KLUČKA, J. *Medzinárodné právo verejné (všeobecná a osobitná časť)*. Bratislava : Iura edition, 2008, s. 48–49. Porovnaj napr.: AKEHURST, M. A. *Modern Introduction to International Law*. Sixth Edition. London : Routledge, 1987, s. 1, alebo: BUERGENTHAL, T., MAIER, H. G. *Public International Law In a Nutshell*. St. Paul : West Publishing Co., 1985, s. 2.

¹⁴ KLUČKA, J. *Medzinárodné právo verejné (všeobecná a osobitná časť)* ... cit. dielo, s. 52.

¹⁵ VRŠANSKÝ, P. – VALUCH, J. a kol.: *Medzinárodné právo verejné. Všeobecná časť*. Bratislava : Eurokódex, 2012, s. 50.

svojich noriem aj viesť medzinárodné spoločenstvo k stabilite a istote v ich vzájomných vzťahoch, riešiť sporné otázky medzi nimi a tiež chrániť ich spoločné záujmy a ciele prostredníctvom spolupráce a priateľských vzťahov.¹⁶

Na základnej úrovni je normatívny systém medzinárodného práva odvodený z prameňov stanovených v čl. 38 ods. 1 štatútu Medzinárodného súdneho dvora, medzi ktoré patria medzinárodné zmluvy, medzinárodná obyčaj, všeobecné právne zásady, súdne rozhodnutia a náuka najviac kvalifikovaných odborníkov rôznych národov.¹⁷ Uvedené ustanovenie štatútu Medzinárodného súdneho dvora je považované za autoritatívny výpočet prameňov medzinárodného práva.¹⁸

Vo vede medzinárodného práva sa možno stretnúť s rôznym výpočtom a vymedzením jednotlivých osobitostí medzinárodného práva, avšak za najpodstatnejšie považujeme osobitnú povahu subjektov a charakteristiku vzťahov medzi nimi. Sumárne medzi podstatné osobitosti tohto právneho odvetvia tak možno radiť subjekty medzinárodného práva a ich vzájomné vzťahy, pramene medzinárodného práva a ich tvorbu a tiež sankčný mechanizmus uplatňovaný v rámci medzinárodného práva.¹⁹ Všetky tieto osobitosti majú vplyv aj na aplikáciu medzinárodného práva, resp. jej rozsah v kybernetickom priestore.

Jedným zo špecifických znakov plne sa prejavujúcim aj v tejto sfére je skutočnosť, že vzťahy v rámci medzinárodného práva sú založené v zásade na koordinačnom, a nie subordinačnom princípe (na rozdiel od vnútroštátneho práva). Štáty ako tradičné subjekty medzinárodného práva spolupracujú v zmysle základných zásad²⁰ a princípov na báze rovnoprávnosti. Koordinačný charakter medzinárodného práva je potom zdôraznený práve tým, že suverénne štáty majú plnú normotvornú spôsobilosť, čo znamená, že nielenže užívajú práva a plnia povinnosti vyplývajúce z medzinárodného práva, ale spoločne s inými štátmi tieto práva a povinnosti aj vytvárajú.²¹ Z toho vyplýva, že medzinárodné právo je právom kompromisu, pričom normatívna kvalita pravidla medzinárodného práva závisí od miery kompromisu, ktorý bol potrebný na jej prijatie.²² Táto skutočnosť sa v plnej miere prejavuje aj v súvislosti s nazeraním na vzťah medzinárodného práva a kybernetického priestoru.

¹⁶ DAVID, V. – BUREŠ, P. – FAIX, M. – SLADKÝ, P. – SVAČEK, O. *Mezinárodní právo veřejné s kazuistikou*. 2 aktualizované a přepracované vydání. Praha: Leges, 2011, s. 77.

¹⁷ CRAWFORD, J. *Brownlie's principles of Public International law*, 8th Edition. Oxford: Oxford University Press, 2012, s. 6.

¹⁸ GRANT, J. P. – BARKER, J. C. *Parry & Grant Encyclopaedic Dictionary of International Law*. Third edition ... cit. dielo, s. 559; Porovnaj: čl. 38 ods. 1 štatútu Medzinárodného súdneho dvora: „Dvor, ktorého úlohou je rozhodovať predložené spory podľa medzinárodného práva, berie za podklad svojho rozhodovania: a) medzinárodné zmluvy, či už všeobecné alebo partikulárne, ustanovujúce pravidlá výslovne uznané štátmi v spore, b) medzinárodnú obyčaj ako dôkaz všeobecnej praxe prijímanej za právo, c) všeobecné právne zásady uznané civilizovanými národmi, d) s výhradou ustanovenia čl. 59 súdne rozhodnutia a náuku najkvalifikovanejších odborníkov rôznych národov ako pomôcku pri určovaní právnych pravidiel.“

¹⁹ KLUČKA, J. *Medzinárodné právo verejné (všeobecná a osobitná časť)* ... cit. dielo, s. 53.

²⁰ Základné zásady medzinárodného práva sú kodifikované v Deklarácii zásad týkajúcich sa priateľských vzťahov a spolupráce medzi štátmi, ktorú prijalo Valné zhromaždenie OSN v roku 1970; Rez. VZ OSN č. 2526/XXV.

²¹ VRŠANSKÝ, P. – VALUCH, J. a kol. *Medzinárodné právo verejné. Všeobecná časť* ... cit. dielo, s. 51.

²² Tamtiež, s. 52.

Vzt'ah kybernetického priestoru a medzinárodného práva

Napriek tomu, že pokrok vedy a techniky je zjavný, nejde o prvý kontakt medzinárodného práva s technologickým pokrokom. Už predchádzajúce obdobie nám ponúka minimálne dva príklady, keď bolo medzinárodné právo podobne náhlým spôsobom konfrontované s výdobytkami doby. Išlo o kontakt s rádiovými vlnami prekračujúcimi hranice a s ľudskou schopnosťou dosiahnuť mimozemské telesá. V každom prípade však bolo považované za samozrejmosť, že aj takého správanie človeka podliehalo existujúcim normám medzinárodného práva.²³

Momentálne sa už dlhšie diskutuje o aplikovateľnosti medzinárodného práva v kybernetickom priestore. Väčšina západných krajín sa už dávnejšie prikláňala k aplikácii existujúceho medzinárodného práva aj v tomto type priestoru, kým niektoré ďalšie, ako napr. Rusko a Čína preferovali špecifickú úpravu a navrhovali osobitnú sústavu noriem. Dnes však už možno povedať, že je to všeobecne uznávaná aplikácia medzinárodného práva. Týmto sa zaoberala aj správa skupiny vládnych expertov zriadenej Valným zhromaždením OSN z roku 2013, ktorá uvádza, že medzinárodné právo a najmä Charta OSN je použiteľná a nevyhnutná na udržanie mieru a stability a podporu otvoreného, bezpečného, mierového a dostupného prostredia informačných a komunikačných technológií.²⁴ Skupina pozostávala zo zástupcov 15 krajín vrátane Spojených štátov amerických, Ruska a Číny. Vo svojej neskoršej správe z roku 2015 odporučili aj súbor noriem týkajúcich sa správania štátov v kybernetickom priestore.²⁵

Tieto by mali v súlade s Chartou OSN a všeobecne uznávanými normami upravujúcimi medzinárodné vzťahy obsahovať okrem iného aj nasledujúce záväzky:

- nevyužívať informačné a komunikačné technológie ani informačné a komunikačné siete na vykonávanie činností, ktoré sú v rozpore s úlohou zachovania medzinárodného mieru a bezpečnosti;
- nevyužívať informačné a komunikačné technológie ani informačné a komunikačné siete na zasahovanie do vnútorných záležitostí iných štátov alebo s cieľom narušiť ich politickú, ekonomickú a sociálnu stabilitu;
- spolupracovať v boji proti trestnej činnosti a teroristickým aktivitám v tejto oblasti;
- uznanie, že práva jednotlivca v *offline* prostredí musia byť chránené aj v *online* prostredí;
- pomoc rozvojovým krajinám pri posilňovaní kapacít v oblasti informačnej bezpečnosti a preklenutí digitálnej priepasti;
- podpora všestrannej spolupráce v tejto oblasti;

²³ ZIMMERMANN, A. *International Law and 'Cyber Space'*. Dostupné na: <http://www.esil-sedi.eu/node/481> (navštívené dňa 19. 09. 2016).

²⁴ United Nations, General Assembly, Group of Governmental Experts (GGE): Report on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013.

²⁵ STINISSEN, J. A Legal Framework for Cyber Operations in Ukraine. In GEERS K. (Ed.) *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn : NATO CCD COE Publications, 2015, s. 124.

- urovnať prípadné spory vyplývajúce z tohto dokumentu mierovými prostriedkami a zdržať sa hrozby silou alebo použitia sily.²⁶

Zároveň však vzniká rovnako vážna otázka, ako aplikovať toto medzinárodné právo v danej sfére? Toto pravdepodobne nie je otázka, ktorá bude záväzným spôsobom vyriešená teraz, ani v blízkej budúcnosti.²⁷

Z uvedeného však vyplýva, že rovnako ako v predchádzajúcich prípadoch, aj aktivity v kybernetickom priestore sa riadia medzinárodným právom ako takým a v prípade, že neexistuje pravidlo zakazujúce správanie v určitej oblasti, štáty si ponechávajú slobodu konať. Zároveň však treba doplniť, že tak ako v predošlých prípadoch je dôsledkom nedostatku v súčasnosti viac špecifických pravidiel, že len základné a všeobecné normy medzinárodného práva upravujú kybernetické aktivity vrátane konceptov, ako sú jurisdikcia a pripísateľnosť správania. S ohľadom na neurčitost' niektorých týchto všeobecných pravidiel, ich neprimeranosť vo vzťahu ku kybernetickým aktivitám, ako aj nedostatok všeobecne akceptovaných, účinných a na pravidlách založených medzištátnych riadiacich štruktúr, predstavuje kybernetický priestor veľkú výzvu pre medzinárodné právo v jeho súčasnej podobe.²⁸

To však nič nemení na skutočnosti, že napr. aj NATO dnes uznáva, že medzinárodné právo vrátane medzinárodného humanitárneho práva a Charty OSN sa aplikuje v kybernetickom priestore.²⁹

Relevantné budú teda najmä všeobecné pravidlá medzinárodného práva. Pozornosť venujeme najmä konceptu *due diligence* (princíp náležitej starostlivosti), ktorý by mal nájsť uplatnenie aj v súvislosti s kybernetickým priestorom.

Tento koncept býva niekedy označovaný aj ako „povinnosť ostráživosti“ či „povinnosť prevencie“. Medzinárodná expertná skupina pracujúca na tallinnskom manuále 2.0 prijala pojem *due diligence* vo svetle bežného používania, no stotožnila sa aj s tým, že môže ísť o synonymum k pojmu „povinnosť ostráživosti“. Odmietla však spojenie s pojmom „povinnosť prevencie“, pretože princíp náležitej starostlivosti nezahŕňa podľa tejto skupiny povinnosť prijať materiálne preventívne opatrenia, aby sa zabezpečilo, že územie štátu nebude využívané v rozpore s týmto princípom. Konštatovali, že tento princíp sa už dlhodobo odráža v judikatúre, pričom ide o všeobecný princíp, ktorý bol špecifikovaný v špecializovaných režimoch medzinárodného práva. V tejto súvislosti sa opreli o prístup Medzinárodného súdneho dvora v posudku k nukleárnym zbraňam³⁰, a keďže

²⁶ Porovnaj: United Nations, General Assembly, Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, A/69/723, 2015.

²⁷ STINISSEN, J. *A Legal Framework for Cyber Operations in Ukraine* ... cit. dielo, s. 124.

²⁸ ZIMMERMANN, A. *International Law and 'Cyber Space'* ... cit. dielo, dostupné na: <http://www.esil-sedi.eu/node/481>.

²⁹ „Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace.“ Wales Summit Declaration (Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales), 5 September 2014, ods. 72.

³⁰ *Nuclear Weapons advisory opinion*: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, I.C.J. 226 (8 July), ods. 39.

aj nové technológie podliehajú existujúcemu medzinárodnému právu, dospeli k záveru, že princíp náležitej starostlivosti možno aplikovať aj v kybernetickom priestore.³¹

Za akúsi všeobecne uznávanú definíciu princípu náležitej starostlivosti možno považovať jeho vymedzenie Medzinárodným súdnym dvorom v prípade Korfský prielav.³² V tomto prípade bolo konštatované, že je povinnosťou každého štátu nepripustiť vedome, aby bolo jeho územie využívané na akty poškodzujúce práva iných štátov. Toto pravidlo je založené na princípe všeobecného medzinárodného práva, že štáty musia vykonávať náležitú starostlivosť pri zabezpečovaní toho, aby územie a objekty, nad ktorými majú suverenity, neboli zneužitá na poškodenie iných štátov. Možno povedať, že je to štandard správania očakávaný od štátov pri dodržiavaní tohto princípu. Tento princíp sa odráža v pravidlách a ich výklade v mnohých špecializovaných režimoch medzinárodného práva. Zjednodušene povedané, ide o povinnosť štátov kontrolovať aktivity na svojom území.³³

Uvedené pravidlo zaväzuje štáty, aby zabezpečili, že ich územie (vrátane kybernetického priestoru – súvisiacej infraštruktúry umiestnenej na ich území) nie je využívané na úkony, ktoré nezákonne poškodzujú iné štáty.³⁴ Práve v súvislosti s aplikáciou tohto všeobecne uznávaného konceptu na kybernetický priestor sa však vynárajú ďalšie otázky týkajúce sa obsahu príslušných povinností. Otázky napr. znejú: spadá aj tranzitný štát (t. j. štát cez ktorý škodlivé dáta prechádzajú) alebo poškodený štát (t. j. štát kde sa škoda zhmotňuje) tiež pod povinnosti vyplývajúce z konceptu *due diligence* a ak áno, do akej miery?³⁵ Ide o právne otázky, na ktoré zatiaľ hľadá medzinárodné spoločenstvo všeobecne akceptovanú odpoveď, pretože v tejto oblasti (ako i v mnohých ďalších) je náročné nájsť zhodu.

Táto povinnosť sa uplatňuje na celom zvrchovanom území štátu. Zahŕňa akúkoľvek počítačovú infraštruktúru, ktorá sa používa, ako aj osoby, ktoré vykonávajú počítačové operácie na tomto území. Zároveň treba mať na zreteli, že strana, ktorá spustila príslušnú kybernetickú operáciu, ju môže vykonávať na diaľku z tretieho štátu. Ako príklad možno uviesť skupinu hekerov v štáte A, ktorá vykonáva deštruktívne kybernetické operácie proti štátu B, využívajúc kybernetickú infraštruktúru štátu C. Ak štát C o tomto vie a neprijme vhodné opatrenia na ukončenie týchto operácií, je to v rozpore s uvedeným princípom *due diligence*.³⁶

³¹ Tallinn Manual 2.0, s. 31-32.

³² *Corfu Channel judgment*: Corfu Channel Case (UK v. Albania), 1949 ICJ 4 (9 April); išlo o prípad, keď dva britské torpédoborce sprevádzajúce britské obchodné lode narazili v albánskych pobrežných vodách Korfského prielavu na míny. Následkom bola smrť a zranenie viacerých britských námorníkov. Spojené kráľovstvo sa obrátilo so žalobou na Medzinárodný súdny dvor, pričom žiadalo náhradu škody s argumentom, že Albánsko o minách muselo vedieť a zanedbalo svoju povinnosť informovať o tom iné štáty. Albánsko ako protiargument uviedlo, že Spojené kráľovstvo prítomnosťou torpédoborcov narušilo suverenity ich pobrežného mora. MSD okrem iného konštatoval, že Albánsko porušilo svoje záväzky založené na určitých všeobecne uznaných zásadách ... a záväzok každého štátu vedome nepripustiť, aby jeho územie bolo využívané na konania, ktoré sú v rozpore s právnymi záujmami iných štátov ... Bližšie pozri: BUCHTA, T. – SÝKOROVÁ, M. *Najdôležitejšie rozsudky v medzinárodnom práve verejnom*. Bratislava : C. H. Beck, 2016, s. 13-14.

³³ Tallinn Manual 2.0, s. 30.

³⁴ ZIMMERMANN, A. *International Law and 'Cyber Space'* ... cit. dielo, dostupné na: <http://www.esil-sedi.eu/node/481>.

³⁵ Tamtiež.

³⁶ Tallinn Manual 2.0, s. 32.

Medzinárodná expertná skupina dospela tiež k záveru, že povinnosť náležitej starostlivosti sa uplatňuje, keď predstavuje kybernetická operácia medzinárodne protiprávny akt. Ako príklad poslúži činnosť štátu A, ktorý monitoruje vládne databázy štátu B formou kybernetickej špionáže tak, že využíva infraštruktúru štátu C. Na štát C sa v tomto prípade nevzťahuje povinnosť náležitej starostlivosti vo forme ukončenia operácií štátu A, pretože špionáž ako taká nie je v rozpore s medzinárodným právom.³⁷ Spomedzi názorov na špionáž možno uviesť vyjadrenie autorov G. P. Corna a R. Taylora, ktorí uvádzajú, že je všeobecne uznávané, že štáty majú nespochybniteľnú právomoc zakázať kybernetickú špionáž na svojom území prostredníctvom vnútroštátneho práva, ale je tiež všeobecne známe, že medzinárodné právo špionáž samu osebe nezakazuje.³⁸

Obdobným je prípad, keď dochádza konaním k porušeniu povinnosti, ktorú má štát vykonávajúci kybernetické operácie proti cieľovému štátu, avšak nie je porušený žiadny záväzok, ktorý by mal k cieľovému štátu teritoriálny štát. Príkladom je bilaterálna medzinárodná zmluva zaväzujúca štáty A a B, aby sa proti sebe navzájom zdržali špionáže. Napriek tomu štát A využíva kybernetickú infraštruktúru štátu C, aby sa zapojil do kybernetickej špionáže proti štátu B spôsobom, ktorý by inak neporušoval medzinárodné právo. Štát C nie je povinný na základe princípu *due diligence* ukončiť operácie štátu A, pretože nie je zmluvnou stranou uvedenej dvojstrannej dohody a špionáž ako taká nepredstavuje porušenie medzinárodného práva.

Expertná skupina sa tiež priklonila k záveru, že len kybernetické operácie vykonávané alebo pripísateľné štátom porušujú suverenitu štátu alebo zákaz používania sily. Napriek tomu sa podľa nich princíp *due diligence* vzťahuje aj na kybernetické operácie vykonávané neštátnymi aktérmi, ktoré síce neporušujú medzinárodné právo samo osebe, ale majú za následok vážne nepriaznivé dôsledky a zasahujú do práva cieľového štátu.³⁹ Uvedené má súvis s rastúcim nebezpečenstvom zo strany neštátnych aktérov aj vo vzťahu k jednotlivým štátom.

Princíp náležitej starostlivosti teda vyžaduje, aby štát prijal všetky opatrenia, ktoré sú za daných okolností uskutočniteľné s cieľom skončiť kybernetické operácie, ktoré zasahujú do práv iných štátov, resp. predstavujú pre ne vážne nepriaznivé následky. K porušeniu tohto princípu dochádza opomenutím, pričom nejde v tejto súvislosti len o nečinnosť, ale aj o prijatie neúčinných alebo nedostatočných opatrení, keď sú dostupné a uskutočniteľné iné vhodnejšie opatrenia. Príkladom takéhoto porušenia je štát, ktorý je nečinný napriek tomu, že na jeho území využíva kybernetickú infraštruktúru teroristická skupina na vykonanie kybernetickej operácie proti inému štátu. Rovnako je však porušením tohto princípu aj stav, keď štát po dôveryhodnom oznámení od iného štátu, že takáto činnosť na jeho území prebieha, nevyčerpá uskutočniteľné opatrenia na jej skončenie.⁴⁰

³⁷ Tallinn Manual 2.0, s. 34-35.

³⁸ CORN, G. P. – TAYLOR, R. Sovereignty in the Age of Cyber. In AJIL Unbound, 2017, Vol. 111, s. 209; dostupné na: <https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-the-age-of-cyber/02314DFCFE00BC901C95FA6036F8CC70> (navštívené dňa 28. 12. 2018); porovnaj: SCHMITT, M. N. – VIHUL, L. Respect for Sovereignty in Cyberspace. In Texas Law Review, 2017, Vol. 95, s. 1643.

³⁹ Tallinn Manual 2.0, s. 34-35.

⁴⁰ Tallinn Manual 2.0, s. 43.

Pohľad Spojených štátov amerických na otázky týkajúce sa aplikácie medzinárodného práva v kybernetickom priestore bol predmetom analýzy, ktorú prezentoval na medzinárodnej konferencii⁴¹ v roku 2012 prof. H. H. Koh.⁴² Svoju prednášku rozdelil na tri časti, pričom prvá niesla názov Medzinárodné právo v kybernetickom priestore: čo vieme a obsahovala desať otázok a odpovedí. Stručne na tomto mieste priblížime jeho závery:

1) Napriek tomu, že nemusí ísť nutne o všeobecne prijímaný názor v rámci medzinárodného spoločenstva, Spojené štáty uznávajú, že ustálené zásady medzinárodného práva je možné aplikovať aj v kybernetickom priestore.

2) Kybernetický priestor nie je bezprávnou zónou, kde môže ktokoľvek vykonávať nepriateľské aktivity bez pravidiel a obmedzení.

3) Kybernetické aktivity môžu za určitých okolností predstavovať použitie sily v zmysle čl. 2 ods. 4 Charty OSN a obyčajového medzinárodného práva.⁴³

4) Právo štátu na sebaobranu, uvedené v čl. 51 Charty OSN, môže byť vyvolané aj aktivitami počítačovej siete, ktoré predstavujú ozbrojený útok alebo jeho bezprostrednú hrozbu.

5) V kontexte ozbrojeného konfliktu sa právo ozbrojeného konfliktu aplikuje aj na reguláciu použitia kybernetických nástrojov pri nepriateľských akciách, rovnako ako pri iných nástrojoch. Princípy nutnosti a proporcionality limitujú použitie sily v sebaobrane a upravujú aj to, čo môže za daných okolností predstavovať zákonnú reakciu.

6) Princíp rozlišovania medzi vojenskými a nevojenskými cieľmi (obsiahnutý v *ius in bello*) sa v kontexte ozbrojeného konfliktu aplikuje aj na útoky v rámci počítačových sietí.

7) Princíp proporcionality (obsiahnutý v *ius in bello*) sa vzťahuje aj na útoky v počítačovej sieti vykonávané v rámci ozbrojeného konfliktu.

8) Štáty by mali vykonať právnu analýzu svojich zbraní vrátane tých, ktoré majú kybernetickú spôsobilosť. Táto by mala obsahovať zistenie, či sú prirodzene nediskriminačné, resp. či je ich použitie v súlade s princípom rozlišovania a proporcionality.

9) Štáty vykonávajúce aktivity v kybernetickom priestore musia brať do úvahy suverenity iných štátov, a to aj mimo kontextu ozbrojených konfliktov.

10) Štáty sú právne zodpovedné za činnosti osôb, ktoré konajú na základe inštrukcií štátu, pod jeho vedením alebo kontrolou.

Druhá časť prednášky mala názov Medzinárodné právo v kybernetickom priestore: výzvy a neistoty. V tejto časti okrem iného pripomenul, že pravidlá *ius ad bellum* sú podľa názoru Spojených štátov aplikovateľné aj na použitie sily v kybernetickom priestore. Podľa prof. Koha ani náročnosť dosiahnutia definitívneho právneho záveru alebo konsenzu medzi štátmi o tom, kedy nepriateľské kybernetické akcie predstavujú ozbrojený útok,

⁴¹ 18. september 2012, the USCYBERCOM Inter-Agency Legal Conference on the Roles of Cyber in National Defence, at Fort Meade, Maryland.

⁴² Právny poradca (U. S. Department of State); Profesor medzinárodného práva (Yale Law School).

⁴³ Ako príklady kybernetickej aktivity, ktorá by mohla predstavovať použitie sily, prof. Koh uvádza: a) operácie, ktoré spôsobia zlyhanie jadrových zariadení; b) operácie, ktoré spôsobia deštrukciu priehrad nad osídlenými oblasťami; alebo c) operácie, ktoré narušia riadenie letovej prevádzky a spôsobia nehodu lietadla.

neznamená, že potrebujeme úplne nový právny rámec špecifický pre kybernetický priestor. V súvislosti s dvojitém užívaním infraštruktúry kybernetického priestoru (armádou štátu a civilným sektorom) uviedol, že vojnové právo vyžaduje, aby civilná štruktúra nebola využívaná na „imunizáciu“ vojenských objektov pred útokom (vrátane kybernetickej oblasti) a každá situácia si bude vyžadovať starostlivú právnu analýzu. Ako ďalšiu naznačil otázku pripísateľnosti správania v kybernetickom priestore, pričom zdôraznil, že vo viacerých ohľadoch ide o otázku viac technickú a politickú než čisto právnu.

V tretej časti, ktorá niesla názov Úloha medzinárodného práva v rozumnom silovom prístupe ku kybernetickému priestoru, konštatoval, že medzinárodné humanitárne právo nie je jediným medzinárodným právom aplikovateľným v kybernetickom priestore. Existujú ďalšie oblasti a normy tak medzinárodného, ako i vnútroštátneho práva, ktoré sa týkajú ľudských práv,⁴⁴ medzinárodného obchodu, kybernetických zločinov a pod., ktoré môžu nájsť vyjadrenie aj v rámci kybernetického priestoru. Na záver konštatoval, že medzinárodné právo nepredstavuje len obmedzenia, ale umožňuje zároveň vykonávať činnosti, ktoré by boli len ťažko predstaviteľné bez toho, aby boli právne legitímne. Rešpektovanie noriem medzinárodného práva preto umožňuje vláde Spojených štátov správať sa v kybernetickom priestore viac legitímne ...⁴⁵

Ius ad bellum a ius in bello

Doposiaľ bolo viac právnych otázok súvisiacich s činnosťou v kybernetickom priestore rozpracovaných v súvislosti s „kybernetickou vojnou“, a teda z hľadiska *ius ad bellum* a *ius in bello*. Osobitnú výzvu existujúcemu medzinárodnému právu predstavujú totiž pravidlá týkajúce sa samotného kybernetického konfliktu. V súčasnosti v tejto oblasti neexistuje úplná zhoda medzi predstaviteľmi národov. Zaujímavé je, že v rámci práce Skupiny vládnych expertov v roku 2015, ktorá mala skúmať otázku aplikácie medzinárodného práva na kybernetický konflikt,⁴⁶ sa táto téma ukázala ako najnáročnejšia. Nezhody prevládajú medzi Ruskom, Čínou a niekoľkými ďalšími krajinami na jednej strane a členskými štátmi NATO na strane druhej. Jadrom rozporu bolo uplatňovanie osobitných ustanovení Charty OSN⁴⁷, a to najmä použiteľnosť čl. 2 ods. 4 (vzdanie sa použitia sily) a čl. 51 (prirodzené právo na sebaobranu).

⁴⁴ K problematike ľudských práv pozri bližšie napr.: SVÁK, J. *Ochrana ľudských práv v troch zväzkoch*. I. zväzok. Bratislava : Eurokódex, 2011.

⁴⁵ KOH, H. H. *International Law in Cyberspace*, online. Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012, dostupné na: <http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf>, (navštívené dňa 28. 12. 2018); porovnaj: MRÁZEK, J. *Mezinárodní právo v kybernetickém prostoru*. In *Právník* 7/2014, roč. 153, s. 555-557; k uvedenej problematike pozri tiež: VRŠANSKÝ, P. – BEDNÁR, D. *Cyber security and the international law*. In *Bratislava Law Review*. Roč. 1, č. 2 (2017), s. 38-49.

⁴⁶ Group of Governmental Experts: Report on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, UNODA, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (navštívené dňa 16. 09. 2016).

⁴⁷ Všeobecná použiteľnosť charty bola odsúhlasená v rámci predchádzajúcej práce skupiny – bližšie pozri v ďalšom texte.

Jednou z otázok týkajúcich sa vývoja noriem v oblasti kybernetického konfliktu je, či je možné prekonať normy zakotvené v Charte OSN a medzinárodných dohodách upravujúce priebeh vojny a ozbrojených konfliktov a vytvoriť normy, ktorými by sa riadil tento nový druh konfliktu. Niektorí autori ako jednu z možností, ktoré by mohli viesť k pokroku, uvádzajú rozšírenie záväzkov Charty OSN vyhýbať sa akciám, ktoré ohrozujú územnú celistvosť alebo politickú nezávislosť štátu (obsiahnuté v čl. 2 ods. 4) na výslovne zahrnuté kybernetické akcie.⁴⁸

Pokiaľ ide o vzťah kybernetického útoku k *ius ad bellum*, ako aj *ius in bello*,⁴⁹ mimoriadne významnú úlohu v tejto súvislosti zohráva už spomenutá medzinárodná expertná skupina, ktorá bola prizvaná Centrom výnimočnosti pre oblasť spoločnej kybernetickej obrany spolupracujúcim s NATO za účelom objasnenia uvedeného vzťahu. Výsledkom bol prvý tzv. Tallinnský manuál⁵⁰ vypracovaný v roku 2012. Pozostáva z dvoch častí – časť I je venovaná kybernetickej bezpečnosti a *ius ad bellum* a časť II sa zaoberá *ius in bello* alebo právom ozbrojených konfliktov.⁵¹ K hlavným záverom prezentovaným v tejto súvislosti v uvedenom dokumente patrí napr. konštatovanie, že aj kybernetické operácie môžu predstavovať použitie sily, a to v prípade, že ich rozsah a účinky sú porovnateľné s nekybernetickými operáciami dosahujúcimi úroveň použitia sily.⁵² Potom štát, ktorý je cieľom kybernetickej operácie dosahujúcej úroveň ozbrojeného útoku, môže uplatniť právo na sebaobranu. Pritom záver, či kybernetická operácia predstavuje ozbrojený útok, závisí od jej rozsahu a účinkov.⁵³ Aj v tomto prípade však možno právo na sebaobranu vykonať aj kolektívne.⁵⁴ Kolektívna sebaobrana proti kybernetickej operácii predstavujúcej ozbrojený útok sa vykonáva na požiadanie štátu – obete a v rozsahu tejto žiadosti.⁵⁵

Vo vzťahu k právu ozbrojených konfliktov dospela expertná skupina k záveru, že kybernetické operácie vykonávané v súvislosti s ozbrojeným konfliktom podliehajú právu ozbrojených konfliktov.⁵⁶ O medzinárodný ozbrojený konflikt pôjde v prípade, že sa vyskytnú nepriateľské akcie, ktoré môžu obsahovať alebo byť limitované na kybernetické operácie, medzi dvomi alebo viacerými štátmi.⁵⁷ V tejto súvislosti je vhodné uviesť,

⁴⁸ LEWIS, J. A. Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine. In GEERS, K. (Ed.) Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015, s. 42-43.

⁴⁹ K vzťahu kybernetických útokov a medzinárodného práva bližšie pozri: ŠMIGOVÁ, K. Kybernetické útoky a medzinárodné právo. In Bratislavské právnické fórum 2013. Bratislava : Univerzita Komenského, Právnická fakulta, 2013 s. 1224-1230.

⁵⁰ Tallinn Manual on the International Law Applicable to Cyber Warfare, 2012.

⁵¹ GABRIŠ, T. Cyber Law ... cit. dielo, s. 174, porovnaj: CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence): Tallinn Manual, dostupné na: <https://ccdcoe.org/research.html> (navštívené dňa 13. 09. 2016).

⁵² Tallinn Manual, pravidlo č. 11, s. 45.

⁵³ Tallinn Manual, pravidlo č. 13, s. 54.

⁵⁴ Bližšie pozri čl. 51 Charty OSN, ktorý zakotvuje prirodzené právo na individuálnu alebo kolektívnu sebaobranu.

⁵⁵ Tallinn Manual, pravidlo č. 16, s. 67; porovnaj: ČEPELKA, Č. – ŠTURMA, P. *Mezinárodní právo veřejné*. Praha : Eurolex Bohemia, 2003, s. 647.

⁵⁶ Tallinn Manual, pravidlo č. 20, s. 75.

⁵⁷ Tallinn Manual, pravidlo č. 22, s. 79.

že všeobecne prijaté kritériá existencie medzinárodného ozbrojeného konfliktu, ktoré odrážajú medzinárodné obyčajové právo, vyplývajú zo spoločného čl. 2 Ženevských dohôrov z roku 1949.⁵⁸ Na druhej strane o nemedzinárodný ozbrojený konflikt pôjde v prípade pretrvávajúceho ozbrojeného násillia, ktoré môže zahŕňať alebo byť obmedzené na kybernetické operácie medzi vládnymi ozbrojenými silami a silami jednej alebo viacerých ozbrojených skupín alebo medzi takými skupinami. Konfrontácia musí dosiahnuť minimálnu úroveň intenzity a strany zapojené do konfliktu musia vykazovať minimálny stupeň organizácie. Prvá veta uvedeného vymedzenia je založená na spoločnom čl. 3 Ženevských dohôrov z r. 1949, ktorý odráža medzinárodné obyčajové právo.⁵⁹ Nesmieme pritom zabúdať, že Tallinnský manuál predstavuje výsledok činnosti nezávislých expertov, ktorý však nemá záväzný charakter.

Pripísateľnosť správania

Mimoriadny význam má v tejto súvislosti aj „pripísateľnosť“ správania. Práve v spojitosti s kybernetickými operáciami predstavuje táto problematika skutočnú výzvu. Už z vymedzenia kybernetického priestoru je totiž zrejmé, že ho charakterizuje množstvo aktérov, jednoduchosť prístupu a anonymita. Určenie, kto je zodpovedný za konkrétnu kybernetickú operáciu, je preto mimoriadne náročné a vyvoláva viaceré otázky:

- kto vykonáva kybernetickú operáciu a na akom základe?
- v prípade, že ide o nešťátnych aktérov, nie sú predsa len podporovaní alebo riadení štátom?
- ak áno, o akú mieru zapojenia alebo podpory ide?⁶⁰

Vo všeobecnosti je totiž prijímaný názor, že štát nesie medzinárodnú zodpovednosť za kybernetické aktivity, ktoré sú pripísateľné štátu a predstavujú porušenie medzinárodnoprávného záväzku.⁶¹ Štát totiž zodpovedá za svoje medzinárodné protiprávne akty. Obyčajovú povahu tohto princípu potvrdil vo viacerých prípadoch aj Medzinárodný súdny dvor.⁶² Medzinárodné protiprávny akt je pritom konanie alebo opomenutie, ktoré:

- a) predstavuje porušenie medzinárodnoprávného záväzku vzťahujúceho sa na štát a
- b) je pripísateľný štátu podľa medzinárodného práva.

⁵⁸ Relevantné ustanovenie čl. 2 Ženevských dohôrov z roku 1949 znie: „*Nehľadiac na ustanovenia, ktoré majú nadobudnúť účinnosť už v mieri, bude sa tento dohovor vzťahovať na všetky prípady vyhlásenej vojny alebo akéhokoľvek iného ozbrojeného konfliktu, vzniknutého medzi dvoma alebo viacerými vysokými zmluvnými stranami, i keď vojnový stav nie je uznávaný jednou z nich. Dohovor sa bude taktiež vzťahovať na všetky prípady čiastočnej alebo úplnej okupácie územia niektorej vysokej zmluvnej strany, i keď sa táto okupácia nestretnie s vojenským odporom.*“

⁵⁹ Tallinn Manual, pravidlo č. 23, s. 84

⁶⁰ Bližšie pozri: O'CONNELL, M. E. – ARIMATSU, L. – WILMSHURST, E. *Cyber Security and International Law*, s. 11; dostupné na: <https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf> (navštívené dňa 10. 10. 2017).

⁶¹ Tallinn Manual 2.0, pravidlo č. 14, s. 84.

⁶² Bližšie pozri napr.: prípad Teherán: Tehran Hostages judgment, prípad Nicaragua: Nicaragua judgment, ods. 283, 292; prípad Gabčíkovo – Nagymaros: Gabčíkovo-Nagymaros judgment, ods. 47. Už skôr sa dotkol tohto princípu aj Stály dvor medzinárodnej spravodlivosti, napr. v prípade Wimbledon: Wimbledon judgment, ods. 30, prípad Továreň v Chorzowe: Factory at Chorzow judgment.

Neexistencia jedného z týchto prvkov bráni, aby bol štát braný na zodpovednosť.⁶³ Následne je potrebné uviesť, že kybernetické operácie vykonávané orgánmi štátu alebo osobami alebo subjektmi splnomocnenými vnútroštátnymi právnymi predpismi vykonávať prvky vládnej moci, sú pripísateľné štátu.⁶⁴ Spomedzi všetkých možných variácií pripísateľnosti štátu asi najjasnejším prípadom je, keď sa štátne orgány, ako napr. vojenské alebo spravodajské agentúry, dopúšťajú neoprávnených činov.⁶⁵

Na druhej strane skupina expertov konštatuje, že kybernetické operácie vykonávané neštátnymi aktérmi sú pripísateľné štátu, ak:

- a) sú vykonávané podľa jeho pokynov alebo pod jeho vedením alebo kontrolou; alebo
- b) štát uznáva a prijíma tieto operácie ako svoje vlastné.⁶⁶

Napriek tomu, že vo všeobecnosti nie sú kybernetické operácie súkromných osôb alebo skupín pripísateľné štátu, uvedené ustanovenie korešponduje so znením článkov o zodpovednosti štátu.⁶⁷

Skupina expertov tiež konštatovala, že pokiaľ ide o kybernetické operácie, štát je zodpovedný za:

- a) jeho pomoc alebo asistenciu inému štátu pri páchaní medzinárodne protiprávneho činu, keď štát poskytne pomoc alebo asistenciu vďaka o okolnostiach medzinárodne protiprávneho činu a čin by bol medzinárodne protiprávny, ak by sa tým spáchal;
- b) medzinárodne protiprávny čin iného štátu, ktorý riadi a kontroluje, ak vedenie a kontrola sú vykonávané s vedomosťou o okolnostiach medzinárodne protiprávneho aktu a akt by bol medzinárodne protiprávny, ak by sa tým vykonal; alebo
- c) medzinárodne protiprávny čin, ktorý prinúti spáchať iný štát.⁶⁸

V súvislosti s pripísateľnosťou kybernetických operácií viacerí autori uvádzajú, že je spätá s analýzou na troch úrovniach, pričom často sa uvádza: technická úroveň (ako), operatívna úroveň (čo) a strategická úroveň (kto a prečo).⁶⁹ Ide pritom o náročnú činnosť, keďže uvedené úrovne sa často prekrývajú a ich vymedzenie je mnohokrát nejasné.

Každopádne, zodpovedať vyššie uvedené otázky bude v konkrétnom prípade náročné aj z dôvodu, že zdroj, z ktorého sa kybernetická operácia šíri, môže byť zneužitý iným aktérom bez vedomia správcu či užívateľa.

⁶³ Tallinn Manual 2.0, s. 84.

⁶⁴ Tallinn Manual 2.0, pravidlo č. 15, s. 87.

⁶⁵ Prikladom aktivít plne pripísateľných príslušným štátom sú napr. kybernetické aktivity nasledujúcich inštitúcií: US Cyber Command; Netherlands Defence Cyber Command; French Network and Information Security Agency (ANSSI); Estonian Defence League's Cyber Unit; People's Liberation Army cyber unit; Israel's Unit 8200 a pod. Tamtiež.

⁶⁶ Tallinn Manual 2.0, pravidlo č. 17, s. 94.

⁶⁷ Bližšie pozri: Articles on State Responsibility, čl. 8. Pozri tiež: UN GGE 2013 Report, ods. 23; UN GGE 2015 Report, ods. 28(f). Tamtiež.

⁶⁸ Tallinn Manual 2.0, pravidlo č. 18, s. 100.

⁶⁹ KAUSHIK, A. Attribution In Cyberspace: Beyond The „Whodunnit“. In Globsec: Cyber Security, Globsec Policy Paper, 16. 05. 2018; dostupné na: <https://www.globsec.org/publications/attribution-cyberspace-beyond-whodunnit/> (navštívené dňa 07.02.2019); porovnaj: RID, T. – BUCHANAN, B: Attributing Cyber Attacks. In Journal of Strategic Studies, Vol. 38, Issue 1-2, s. 4-37; dostupné na: <http://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382> (navštívené dňa 07. 02. 2019).

Záver

Kybernetický priestor označovaný aj za piatu doménu na vedenie vojny predstavuje svojím jedinečným charakterom veľkú výzvu pre súčasné medzinárodné právo.⁷⁰ Pod pojmom medzinárodné právo pritom rozumieme medzinárodné právo verejné, ktorého tradičnými subjektmi sú štáty. Samotné medzinárodné právo je pritom právom kompromisu, pričom normatívna kvalita pravidla medzinárodného práva závisí od miery kompromisu, ktorý bol potrebný na jej prijatie,⁷¹ čo sa prejavuje aj v súvislosti s nazeraním na vzťah medzinárodného práva a kybernetického priestoru. Prax nám zároveň ukazuje, že tento kompromis sa vo viacerých otázkach súvisiacich s týmto typom priestoru hľadá zatiaľ veľmi ťažko.

Dnes už je síce aj v ňom všeobecne uznávaná aplikácia medzinárodného práva, avšak v dôsledku nedostatku špecifických pravidiel upravujú kybernetické aktivity len jeho všeobecné normy, ktoré sú často až príliš všeobecné a neprimerané pre tento druh aktivít. Relevantné budú teda najmä všeobecné pravidlá medzinárodného práva, medzi ktoré patrí napr. koncept *due diligence* (princíp náležitej starostlivosti). Už v prípade Korfský prieplyv⁷² z roku 1949 bolo konštatované, že je povinnosťou každého štátu nepripustiť vedome, aby bolo jeho územie využívané na akty poškodzujúce práva iných štátov. Z toho vyplývajúci princíp náležitej starostlivosti potom vyžaduje, aby štát prijal všetky opatrenia, ktoré sú za daných okolností uskutočniteľné, s cieľom skončiť kybernetické operácie na jeho území, ktoré zasahujú do práv iných štátov.

Skutočnou výzvou v tejto súvislosti je problematika pripísateľnosti správania, pretože už z vymedzenia kybernetického priestoru je zjavné, že ho charakterizuje množstvo aktérov, jednoduchosť prístupu a anonymita.

Medzinárodné spoločenstvo tak stojí pred viacerými skutočne relevantnými otázkami, z ktorých mnohé nebudú pravdepodobne záväzným spôsobom vyriešené ani v blízkej budúcnosti.

Literatúra

- AKEHURST, M. *A Modern Introduction to International Law.*, Sixth Edition. London : Routledge, 1987
- BUERGENTHAL, T. – MAIER, H. G. *Public International Law In a Nutshell.* St. Paul : West Publishing Co., 1985
- BUCHTA, T. – SÝKOROVÁ, M. *Najdôležitejšie rozsudky v medzinárodnom práve verejnom.* Bratislava : C. H. Beck, 2016
- CORN, G. P. – TAYLOR, R. Sovereignty in the Age of Cyber. In *AJIL Unbound*, 2017, Vol. 111, s. 207-212
- CRAWFORD, J. *Brownlie's principles of Public International law.* 8th Edition. Oxford : Oxford University Press, 2012
- ČEPELKA, Č. – ŠTURMA, P. *Mezinárodní právo veřejné.* Praha : Eurolex Bohemia, 2003
- DAVID, V. – BUREŠ, P. – FAIX, M. – SLADKÝ, P. – SVAČEK, O. *Mezinárodní právo veřejné s kazuistikou.* 2. aktualizované a přepracované vydání. Praha : Leges, 2011

⁷⁰ Bližšie pozri: ZIMMERMANN, A. *International Law and 'Cyber Space'* ... cit. dielo, dostupné na: <http://www.esil-sedi.eu/node/481>.

⁷¹ VRŠANSKÝ, P. – VALUCH, J. a kol. *Medzinárodné právo verejné. Všeobecná časť* ... cit. dielo, s. 52.

⁷² *Corfu Channel judgment.*

- GÁBRIŠ, T. *Cyber Law*. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2014
- GRANT, J. P. – BARKER, J. C. *Parry & Grant Encyclopaedic Dictionary of International Law*. Third Edition. Oxford : Oxford University Press, 2009
- JASPERS, K. (Elexová, P. preklad): *Malá škola filozofického myslenia*. Bratislava : Kalligram, 2003
- KAUSHIK, A. Attribution. In *Cyberpace: Beyond The „Whodunnit“*. In Globsec: Cyber Security; Globsec Policy Paper, 2018
- KLUČKA, J. *Medzinárodné právo verejné (všeobecná a osobitná časť)*. Bratislava : Iura edition, 2008
- KNORR, A. The Stability of Cyberspace. In POLČÁK, R. – ŠKOP, M. – ŠMAHEL, D. (Ed.) *Cyberspace 2005*. Brno : Masarykova univerzita, 2006
- LEWIS, J. A. Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine. In GEERS K. (Ed.) *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015
- MELKOVÁ, M. – SOKOL, T. Kybernetický priestor ako nová dimenzia národnej bezpečnosti. In *Bezpečnostné fórum 2015*. I. zväzok. Banská Bystrica : Vydavateľstvo Univerzity Mateja Bela – Belianum, 2015
- MELZER, N. *Cyber Warfare and International Law*. UNIDIR Resources, 2011
- MRÁZEK, J. Mezinárodní právo v kybernetickém prostoru. In *Právník 7/2014*, roč. 153, s. 537-561
- RID, T. – BUCHANAN, B. Attributing Cyber Attacks. In *Journal of Strategic Studies*, vol. 38, Issue 1-2, s. 4-37
- SCHMITT, M. N. (General Ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge : Cambridge University Press, 2017
- SCHMITT, M. N. (General Ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge : Cambridge University Press, 2013
- SCHMITT, M. N. – VIHUL, L. Respect for Sovereignty in Cyberspace. In *Texas Law Review*, 2017, vol. 95, s. 1639-1670
- STINISSEN, J. A Legal Framework for Cyber Operations in Ukraine. In GEERS K. (Ed.) *Cyber War in Perspective: Russian Aggression against Ukraine*. NATO CCD COE Publications, Tallinn, 2015
- SVÁK, J. *Ochrana ľudských práv v troch zväzkoch*. I. zväzok. Bratislava : Eurokódex, 2011
- ŠMIGOVÁ, K. Kybernetické útoky a medzinárodné právo. In *Bratislavské právnické fórum 2013*. Bratislava : Univerzita Komenského, Právnická fakulta, 2013, s. 1224-1230
- VRŠANSKÝ, P. – BEDNÁR, D. Cyber security and the international law. In *Bratislava Law Review*. Roč. 1, č. 2 (2017), s. 38-49
- VRŠANSKÝ, P. – VALUCH, J. a kol. *Medzinárodné právo verejné. Všeobecná časť*. Bratislava : Eurokódex, 2012

Dokumenty, prípady a internetové zdroje

- Articles on State Responsibility, čl. 8. Pozri tiež: UN GGE 2013 Report, ods. 23; UN GGE 2015 Report, ods. 28(f)
- CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence): Tallinn Manual, dostupné na: <https://ccdcOE.org/research.html>
- Deklarácia zásad týkajúcich sa priateľských vzťahov a spolupráce medzi štátmi, 1970; Rez. VZ OSN č. 2526/XXV
- Global Cybersecurity Index 2017*, Geneva : International Telecommunication Union, 2017; materiál dostupný na: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf,
- Group of Governmental Experts: Report on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, UNODA, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
- Internet World Stats, dostupné na: <https://www.internetworldstats.com/stats.htm>
- KOH, H. H. International Law in Cyberspace, online. - Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012, dostupné na: <http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf>,

- O'CONNELL, M. E., ARIMATSU, L., WILMSHURST, E.: Cyber Security and International Law; dostupné na: <https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf>
- Poradný posudok k jadrovým zbraňam: *Nuclear Weapons advisory opinion*: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, I.C.J. 226 (8 July)
- Prípád Gabčíkovo-Nagymaros: Gabčíkovo-Nagymaros judgment: Gabčíkovo-Nagymaros Project (Hung. V. Slovakia), 1997, ICJ 7 (25 September)
- Prípád Korfu: *Corfu Channel judgment*: Corfu Channel Case (UK v. Albania), 1949 ICJ 4 (9 April)
- Prípád Nicaragua: Nicaragua judgment: Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA) 1986, I. C. J. Reports (27 June)
- Prípád Teherán: Tehran Hostages judgment: United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), 1980, ICJ 3 (24 May)
- Prípád Továreň v Chorzowe: Factory at Chorzow judgment: Factory at Chorzow (Ger. v. Pol.), merits, 1928, PCIJ (ser. A), No. 17 (13 September)
- Prípád Wimbledon: Wimbledon judgment: Wimbledon judgment (United Kingdom v. Germany), 1923, PCIJ (ser. A.) No. 1 (17 August)
- Štatút Medzinárodného súdneho dvora
- TSAGOURIAS, N. The legal status of cyberspace. In Research Handbook on International Law and Cyberspace, dostupné na: <http://www.e-elgar.com/shop/eep/preview/book/isbn/9781782547396/>
- United Nations, General Assembly, Group of Governmental Experts (GGE): Report on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013.
- United Nations, General Assembly, Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, A/69/723, 2015.
- Wales Summit Declaration (Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales), 5 September 2014,
- ZIMMERMANN, A. International Law and 'Cyber Space', dostupné na: <http://www.esil-sedi.eu/node/481>
- Ženevské dohovory z roku 1949