Oponentský posudok

na habilitačnú prácu JUDr. Jozef Valuch, PhD.: Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti

Oponentský posudok bol vypracovaný na základe zákona č. 131/2002 Z.z. o vysokých školách a o zmene a doplnení niektorých zákonov a Vyhlášky Ministerstva školstva č. 6/2005 Z.z. o postupe získavania vedecko-pedagogických titulov alebo umelecko-pedagogických titulov docent a profesor.

Zvolená téma práce „Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti“ je vysoko aktuálna, náročná, zložitá, komplexná, interdisciplinárna a mnohorozmerná téma, a to nielen z hľadiska potreby analýzy čiastkových aspektov problematiky kybernetickej bezpečnosti, ale aj z hľadiska vývojového.

Voľba tejto živej témy umožnila autorovi v habilitačnej práci formulovať aktuálne a pre prax zaujímavé odborné stanoviská a názory na súčasnú úpravu de *lege lata* i načrtnúť niektoré úvahy *de lege ferenda*. Súhlasíme s autorom, ktorý v úvode konštatuje, že problematika práce patrí „medzi najaktuálnejšie otázky medzinárodného práva, o čom svedčí aj fakt, že jej je venovaná pozornosť nielen na úrovni jednotlivých štátov, ale i na mnohých fórach, univerzitách či medzinárodných organizáciách v Amerike, Európe i ďalších kontinentoch. V Slovenskej republike je však zatiaľ táto aktuálna téma predmetom len nepatrného množstva vedeckých, či odborných článkov.“ (s. 10).

Aktuálnosť témy potvrdzuje súčasný vývoj medzinárodnej situácie, narastajúce hrozby a útoky v oblasti kybernetickej komunikácie, ktoré ovplyvňujú celkový vývoj medzinárodných vzťahov. Všetky dôsledky kybernetických hrozieb útokov dnes ešte nie je možné s úplnosťou predvídať. Medzinárodné spoločenstvo štátov však musí na uvedené výzvy vznikajúce v oblasti materiálnych prameňov medzinárodného práva reagovať prijímaním nových pravidiel, vrátane zmluvných, obyčajových noriem ako aj formulovaním nových všeobecných zásad medzinárodného práva.

Problematika kybernetických hrozieb je široká, nie je možné ju podrobne analyzovať v rámci jedného písomného výstupu. Na s. 10 autor korektne píše, že „Sme si plne vedomí aktuálnosti a rozsahu danej témy, ktorá neumožňuje na jednom mieste postihnúť všetky súvisiace aspekty v maximálnej detailnej hĺbke.“

Pokiaľ ide o náročnosť skúmanej problematiky, habilitant výstižne zdôrazňuje, že „Náročnosť témy je pritom podčiarknutá skutočnosťou, že viaceré aspekty uvedenej problematiky sú zatiaľ doktrínou vnímané rozdielne.“ (s. 11).

Poznamenávame, že zložitosť témy vyplýva najmä zo zložitosti právnych otázok spojených s pertraktovanou témou. Či už ide o otázky subjektivity, prameňov, pravidiel a zásad, kodifikácie, riešenia sporov, zodpovednosti, sankcií či donútenia.

Mnohé z právnych problémov len čakajú na podrobnejšiu medzinárodnoprávnu úpravu. Keďže ide o živú oblasť skúmania, obsah a závery hodnotenej práce otvárajú priestor pre ďalší výskum rôznych medzinárodnoprávnych aspektov problematiky kybernetických hrozieb a kybernetickej bezpečnosti. K problematike možno pri ďalšom výskume pristupovať nielen z pohľadu na kybernetické hrozby či útoky, ktorými štát porušuje medzinárodné právo, teda z pozície páchateľa, ale aj z pohľadu štátov či medzinárodného spoločenstva štátov, ktoré sa usilujú práve s pomocou kybernetických hrozieb alebo kybernetických útokov odstrániť hrozbu mieru, obnoviť mier alebo zabrániť kybernetickým hrozbám a útočným činom odporujúcim cieľom a zásadám Charty OSN. V tomto zmysle, kybernetická hrozba môže byť nielen hrozná útočná zbraň porušiteľa pravidiel medzinárodného práva, ale aj mimoriadne účinná obranná zbraň tých, čo chránia pravidlá medzinárodného práva pred nežiaducim porušením. V takom prípade, použitie kybernetickej hrozby alebo kybernetický útok budú predstavovať legálne konanie „zlučiteľné s cieľmi Charty OSN“, pretože je zamerané proti konaniu, ktoré je „nezlučiteľné s cieľmi a zásadami Charty OSN“. Bezpečnostná rada OSN by takto mohla postupovať v súlade s jej kompetenciami podľa kapitoly VI článku 36 ods. 1 Charty OSN (kybernetická hrozba ako odporúčaný prostriedok mierového urovnania sporu), kapitoly VII článkov 39-43 (kybernetická hrozba (varovanie) ako odporúčaný prostriedok donútenia bez použitia sily), alebo aj podľa článku 51 charty (kybernetická hrozba alebo útok ako akt sebaobrany). Tak isto podľa kapitoly VIII článku 52 Charty OSN (kybernetická hrozba alebo útok ako regionálny prostriedok na zachovanie mieru a bezpečnosti). Zaujímavý priestor pre výskum ponúka aj otázka využitia kybernetickej hrozby v súvislosti s otázkou medzinárodnoprávnej zodpovednosti (kybernetická hrozba ako okolnosť vylučujúca protiprávnosť konania). Medzi tieto okolnosti patrí napríklad použitie kybernetickej hrozby či útoku na základe súhlasu poškodeného štátu, jej použitie vo forme legálneho protiopatrenia, jej aplikácia z dôvodu krajnej núdze, z dôvodu stavu tiesne, z dôvodu pôsobenia vis maior, alebo z dôvodu rešpektovania či ochrany kogentných noriem medzinárodného práva pred porušením a pod. Ďalšou teoreticky uvažovanou možnosťou je možnosť neobmedzeného využitia

kybernetickej hrozby alebo útoku proti „nepriateľským štátom“ na základe 107 Charty OSN (kybernetická hrozba alebo útok ako opatrenie proti „nepriateľským“ štátom). . Zaujímavá je aj otázka ďalšieho výskumu kybernetických hrozieb v súvislosti s vymedzením hlavných obsahových znakov a rozsahu pojmu zločin agresie.

Nemožno pochybovať, že v otázke právnej úpravy kybernetickej hrozby a kybernetickej bezpečnosti vývoj materiálnych prameňov medzinárodného práva ďaleko predbieha vývoj formálnych prameňov medzinárodného práva. Svedčí o tom aj to, že Komisia OSN pre medzinárodné právo sa v súčasnosti nezaoberá otázkou týchto oblastí v rámci kodifikácie alebo pokrokového rozvoja medzinárodného práva. Absencia právnej úpravy na úrovni základných prameňov práva otvára široký priestor pre skúmanie uvedenej problematiky na úrovni pomocných prameňov medzinárodného práva, osobitne náuky medzinárodného práva.

Habilitant v úvode práce (s. 11-12) formuluje hlavný cieľ a parciálne ciele habilitačnej práce. Hlavným cieľom práce je „na základe analýzy, komparácie a ďalších vedeckých metód (...) vymedziť medzinárodnoprávnu povahu kybernetických operácií ako aktuálnej hrozby pre medzinárodnú bezpečnosť. Prvý, parciálny cieľ práce „má prevažne deskriptívnu povahu a spočíva v snahe ozrejmiť na základe relevantných súvislostí pojem a podstatu kybernetických hrozieb a kybernetického priestoru.“ Druhý, analyticky orientovaný parciálny cieľ práce „spočíva v rozbore vzťahu kybernetického priestoru a medzinárodného práva, s ohľadom na princíp suverenity a použitie sily“. Tretí, analyticko-hodnotiaci parciálny cieľ je „na konkrétnych prípadoch zneužitia kybernetického priestoru analyzovať kybernetické operácie a na jednom z nich aplikovať tzv. Schmittovu analýzu.“

Štruktúra habilitačnej práce zodpovedá zámerom autora dosiahnuť vyššie uvedené ciele. Habilitant dôvodí, prečo si zvolil „vlastný prístup a pri koncipovaní práce“, a že sa snažil, „aby jednotlivé kapitoly na seba úzko nadväzovali a boli pokiaľ možno „vstupnou bránou“ nasledujúcim častiam práce.“ (s. 10).

V prvej kapitole (1 Pojmové vymedzenie)(s. 13-49), autor analyzuje nasledovné otázky:1.1 Pojmy týkajúce sa bezpečnosti ; 1.2 Hrozby medzinárodnej bezpečnosti; 1.3 Kybernetické hrozby v 21. storočí; 1.4 Kybernetický priestor; 1.5 Kybernetický útok; 1.6 Pojem a povaha medzinárodného práva.

V druhej kapitole (2 Kybernetický priestor a medzinárodné právo) (s. 50-97) habilitant porovnáva a analyzuje nasledujúce okruhy problémov: 2.1 Vzťah kybernetického priestoru a medzinárodného práva; 2.2 Suverenita štátu a koncept virtuálnych hraníc; 2.2.1 Hranice

suverenity a kybernetický priestor; 2.3 Použitie sily v kybernetickom priestore; 2.3.1 Schmittova analýza; 2.4 Sebaobrana; 2.5 Kybernetická špionáž). Túto kapitolu považujeme za nosnú z hľadiska posudzovania medzinárodnoprávnej úpravy týkajúcej sa otázok kybernetických hrozieb a kybernetickej bezpečnosti.

V tretej kapitole (3 Prípady zneužitia kybernetického priestoru) (s. 98-126) autor analyzuje niektoré konkrétne prípady z medzištátnej praxe, konkrétne 3.1 Estónsko (2007); 3.2 Rusko – Gruzínsky konflikt (2008; 3.3 Irán (2010); a 3.4 Konflikt na Ukrajine (od r. 2013).

Vo štvrtej kapitole (4 Opatrenia vybraných organizácií a SR) (s.127-157) autor rozoberá postup v kontexte relevantných aktivít niektorých medzinárodných vládnych organizácií, konkrétne NATO (4.1); OBSE (4.2) ako aj Slovenskej republiky (4.3). V tejto kapitole sa Zaoberá sa aj Globálnym indexom kybernetickej bezpečnosti v kontexte aktivít Svetového ekonomického fóra.

Pri analýze jednotlivých otázok i celkovom prístupe k spracovaniu autor preukázal hlbšie pochopenie komplexného a interdisciplinárneho charakteru problematiky kybernetickej bezpečnosti. Ako je známe, táto problematika zasahuje nielen do oblasti úpravy medzinárodného práva verejného, medzinárodného práva súkromného, medzinárodného obchodu, medzinárodných vzťahov, vnútroštátneho práva, európskeho práva, ale aj do oblasti teórie a praxe iných spoločenských vied, prírodných vied, či technických vied, ITT, výskumu umelej inteligencie a iných vedných disciplín.

Mnohorozmernosť kybernetických hrozieb možno jednoznačne odvodiť z prejavov minulých, súčasných a odhadovaných budúcich kybernetických hrozieb a útokov, o ktorých sa autor zmieňuje na viacerých miestach tejto zaujímavej práce.

Po formálnej stránke, habilitačná práca spĺňa požiadavky platnej právnej úpravy kladené na práce tohto druhu. po jazykovej a štylistickej stránke. Práca s odbornou literatúrou a vedecká diskusia zodpovedá zámerom autora prezentovať základné poznatky o predmete skúmania v súčasnosti i z hľadiska vývojového.

Pokiaľ ide o metódy spracovania, autor využil - jednotlivo aj kombinovane - viaceré metódy a prostriedky vedeckej práce, na ktoré upozornil v úvode práce (s. 12). Aplikoval najmä metódu právnej analýzy, právnej komparácie, indukcie, právnej syntézy, ďalej systematickú analýzu, jazykový (sémantický) rozbor, logickú metódu ako aj historicko-právnu analýzu.

Po obsahovej stránke habilitačná práca predstavuje prínos do domácej a zahraničnej odbornej diskusie venovanej zložitej problematike medzinárodnoprávnych aspektov kybernetickej bezpečnosti. Obsah práce zodpovedá súčasnému stavu pozitívnoprávnej úpravy a stavu vedeckého poznania v danej oblasti.

Autor zohľadňuje aktuálne trendy v oblasti pokrokového rozvoja medzinárodného práva, teda otázky, ktoré dosiaľ neboli kodifikované v medzinárodnom zmluvnom práve, a ku ktorým neexistuje ani dlhodobá medzištátna prax. Vzhľadom na krátkosť času, medzinárodné obyčajové pravidlá sa iba vytvárajú. Pre ich vznik zatiaľ chýba *usus longaevus a opinio iuris*.

Z prehľadu literatúry vyplýva, že autor sa dobre orientuje v základných a pomocných prameňoch medzinárodnoprávnej úpravy, v najdôležitejších vedeckých a expertných výstupoch, venovaných problematike kybernetických hrozieb.

Habilitant prináša niektoré nové sumarizujúce pohľady na pertraktované otázky.

Napríklad, na s. 28 píše v súvislosťou na hrozby medzinárodnej bezpečnosti, že „Už sme naznačili, že žiadny štát, bez ohľadu na to, aký je vyspelý a silný, nemôže len vlastnými silami účinne vzdorovať týmto hrozbám, pričom nemožno ani predpokladať, že každý štát bude schopný alebo ochotný vlastné obyvateľstvo chrániť a brať pritom ohľad a nespôsobovať škody svojim susedom."

Na záver prvej kapitoly na s. 47 formuluje záver, že „V posledných rokoch sme totiž viac ako kedykoľvek predtým svedkami toho, že sa mení priestor operácií, použitá „munícia" a tiež ciele. Dôkazom týchto zmien je presun množstva aktivít do kybernetického priestoru."

Na s. 59 upresňuje, v súvislosti so zodpovednosťou, že „Rovnaký význam má v tejto súvislosti aj „pripísateľnosť" správania. Práve v spojitosti s kybernetickými operáciami predstavuje táto problematika skutočnú výzvu. Už pri vymedzení kybernetického priestoru sme totiž uviedli, že ho charakterizuje množstvo aktérov, jednoduchosť prístupu a anonymita."

Zaujímavá je celá časť práce venovaná osvetleniu odbornej diskusie venovanej obsahu a rozsahu pojmu „kybernetický priestor", vrátane otázky jeho „neteritoriálnej povahy" z dôvodu, že podľa niektorých autorov, ide o „*res communis omnium*" (napr. s. 69)

Na s. 72 autor správne píše, že „Ako sme už naznačili, samotná suverenita nie je absolútna, čo znamená, že neumožňuje danému štátu konať bez ohľadu na medzinárodné právo."

V súvislosti s kybernetickou špionážou v kybernetickom priestore autor píše na s. 90, že „Práve charakteristické črty tohto typu priestoru, ktoré sme spomínali v prvej časti tejto práce (anonymita, globálny rozmer „bez hraníc“, jednoduchý prístup) sú „prednosťami“, ktoré môže využívať tento typ správania.“

Na s. 92 autor najprv prorocky a potom realisticky konštatuje, v súvislosti s prípadmi zneužitia kybernetického priestoru, že „Čoraz častejšie sme svedkami udalostí, počas ktorých sa kybernetický priestor stáva dejiskom negatívnych operácií zameraných aj voči štátom. Ani zďaleka však nejde o prvé a žiaľ zrejme ani o posledné takéto aktivity.“

Pokiaľ ide o právne hodnotenie, možno súhlasiť s odkazom autora uvedeným na Tallinský Manuál na s. 119, že „kybernetické operácie vykonávané v kontexte ozbrojeného konfliktu podliehajú právu ozbrojených konfliktov.“

Zaujímavý je poznatok uvedený na s. 122 , že „V rámci konfliktu na Ukrajine sme zatiaľ deštruktívne účinky kybernetických operácií nezaznamenali.“

Možno konštatovať, že habilitant dobre chápe zvolenú tému a dobre sa v nej orientuje s akcentom na existujúce dostupné materiálne a formálne pramene medzinárodného práva. Pri spracovaní sa opieral aj o dostupné pomocné pramene medzinárodného práva (judikatúra a náuka najviac kvalifikovaných odborníkov na medzinárodné právo).

Pokiaľ ide o judikatúru, autor odkazuje na využiteľné rozhodnutia medzinárodných súdov, napríklad vo veci: Corfu Channel Case (UK v. Alb.), 1949; Factory at Chorzow judgment: Factory at Chorzow (Ger. v. Pol.), merits, 1928; Gabčíkovo-Nagymaros Project (Hung. V. Slovakia), 1997; Island of Palmas (Netherlands v. USA), 1928; The Case of the SS „Lotus“ (France v. Turkey), 1927; Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA) 1986; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, ; Oil Platforms (Iran v. USA), 2003; Reparation for Injuries advisory opinion: Reparation for Injuries Suffered in the Service of the United Nations, 1949; United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), 1980; Wimbledon judgment (United Kingdom v. Germany), 1923.

Argumentácia a vedecká diskusia v práci je založená na autorových vlastných názoroch i citovaných odborných názorov a úvahách iných odborníkov. Autor vhodne aplikuje dostupné prostriedky právnej interpretácie textov s cieľom ešte viac objasniť či spresniť význam v nich použitých výrazov.

Závery práce k jednotlivým kapitolám i záverečná syntéza sú vyargumentované.

Pokiaľ ide o čiastkové závery ku kapitole 2 (s. 93-97), možno súhlasiť s názorom autora, že „Kybernetický priestor, označovaný aj za piatu doménu na vedenie vojny, predstavuje svojim jedinečným charakterom veľkú výzvu pre súčasné medzinárodné právo“. Tak isto so záverom, že absentujú „špecifické pravidlá upravujúce kybernetickú bezpečnosť“, ako aj s o záverom, že „Relevantné budú teda najmä všeobecné pravidlá medzinárodného práva, medzi ktoré patrí napr. koncept due dilligence (princíp náležitej starostlivosti).“ Z hľadiska aplikácie zásady zvrchovanej rovnosti štátov je dôležitý záver, že „Vychádzajúc zo skutočnosti, že kybernetická infraštruktúra je vždy fyzicky umiestnená na určitom type územia, nad ktorým vykonáva kontrolu určitý štát, možno aj v rámci kybernetického priestoru aplikovať princíp suverenity.“(s. 93). Z hľadiska úvah *de lege lata* a *de lege ferenda* je dôležitý záver, že „V súčasnom medzinárodnom práve je už pevne zakotvený nielen zákaz použitia sily ale i hrozby silou, pričom tento zákaz má kogentný charakter. Neexistuje však autoritatívna definícia alebo kritériá pre určenie čo predstavuje "hrozbu" alebo "použitie sily", tak ako neexistuje ani medzinárodný konsenzus o tom, čo predstavuje použitie sily v kybernetickom priestore. Všetko zároveň nasvedčuje tomu, že v dohľadnom čase sa to pravdepodobne ani nezmení.“(s. 94). Habilitant tak isto prikladá veľký význam tzv. Schmittovej analýze,“ ktorá zostáva jedným z najbežnejšie uvádzaných rámcov na charakterizovanie použitia sily v kybernetickom priestore.“ (s. 94). Autor správne poukazuje na prienik relevantnej právnej úpravy s ustanoveniami Charty OSN, keď dospieva k záveru, že „aj kybernetická operácia, ktorá predstavuje hrozbu alebo použitie sily proti územnej celistvosti alebo politickej nezávislosti štátu, alebo ktorá je iným spôsobom nezlučiteľná s cieľmi OSN, je v rozpore s jeho znením.“ (s. 95). Dôležitý je záver autora o tom, že kybernetické operácie „môžu mať teda rôznu povahu, adresátov i účinky. Avšak aj keby nedosiahli úroveň použitia sily, neznamená to automaticky, že sú v súlade s medzinárodným právom. Môžu predstavovať porušenie iných noriem alebo princípov, napr. zákaz zasahovania do vnútorných záležitostí štátu. Skutočnú výzvu však bude predstavovať pripísateľnosť takéhoto správania, nakoľko samotný kybernetický priestor charakterizuje množstvo aktérov, jednoduchosť prístupu a anonymita.“ (s. 96).

Pokiaľ ide o všeobecnú syntézu (s. 158-164), habilitant vyslovuje záver, že „konečným cieľom každého právneho systému - ako vnútroštátneho, tak i medzinárodného - je zaistiť bezpečnosť pre všetky subjekty, ktoré ovláda, či riadi. „Bezpečnosť“ ako taká vo všeobecnosti pritom predstavuje ideálny stav a reálne je možné dosiahnuť len určitú elimináciu hrozieb, ktoré sa neustále vyvíjajú.“(s. 158) Ďalším dôležitým záverom je, že „kybernetický priestor,

označovaný aj za piatu doménu na vedenie vojny, predstavuje svojim jedinečným charakterom veľkú výzvu pre súčasné medzinárodné právo.“ Tak isto, že „Nie každá kybernetická operácia však predstavuje kybernetický útok.“ Pokiaľ ide o medzinárodnoprávne aspekty, autor opätovne zdôrazňuje, že „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 dilligence (princíp náležitej starostlivosti).“ Pokiaľ ide o otázku suverenity, prikláňa sa k názorom, že „ani globalizácia ako taká neprekonala tento inštitút. Namiesto toho dnes pojem „suverenita“ zaujíma ústredné postavenie v diskusiách o normatívnej architektúre kybernetického priestoru“ a že „Existencia suverenity sa predpokladá a v prípade pochybností o jej existencii sa v jej prospech uplatní právna domnienka, zatiaľ čo obmedzenie suverenity sa musí preukázať.“ Podľa autora, „Samotný výkon suverenity môže byť pritom obmedzený obyčajovými alebo zmluvnými pravidlami medzinárodného práva. Je to teda práve suverenita, ktorú má štát nad územím, ktorá ho oprávňuje kontrolovať kybernetickú infraštruktúru a počítačové aktivity na jeho území.“ Dôležitý je záver habilitanta o tom, že „Medzinárodný konsenzus neexistuje ani v otázke, čo predstavuje použitie sily v kybernetickom priestore.“(s. 160). „ Zaujímavý je záver, že „Napriek tomu, že mnohé otázky sú zatiaľ doktrínou vnímané rozdielne, podľa viacerých autorov jednotlivé štáty vo svojom prístupe k nedeštruktívnym kybernetickým operáciám naznačujú, že tieto sú skôr prípustné ako zakázané. Výsledkom môže byť vo všeobecnosti akási budúca „obyčaj prípustnosti“ kybernetických operácií.“ (161). Habilitant považuje v závere práce za vhodné „spomenúť aj predpoklad profesora M. Schmitta o tom, že štáty sa budú pri hodnotení použitia sily v kybernetickom priestore v prvom rade spoliehať na existujúce normy, najmä na čl. 2 ods. 4 Charty OSN. Ako však niektorí predpovedali a Stuxnet potvrdil, čl. 2 ods. 4 Charty OSN bude pravdepodobne slabým obmedzením na ofenzívne kybernetické operácie.“(s. 162) . Autor na záver práce konštatuje, že „Záverom možno dodať, že práve každodenná závislosť na procesoch prebiehajúcich vo virtuálnej rovine, na internete a technických prostriedkoch spôsobuje, že zaistenie kybernetickej bezpečnosti už predstavuje jednu zo základných podmienok fungovania štátu, výkonu jeho funkcií a poskytovania verejných služieb. V súčasnom bezpečnostnom prostredí, za neustáleho pokroku v oblasti vedy a techniky, však predstavuje stav „absolútnej bezpečnosti“ len akúsi „ilúziu“. Na druhej strane je práve medzinárodná spolupráca prostriedkom, ktorým sa dá k tejto „ilúzii“ priblížiť.“ S týmto postrehom habilitanta možno tak isto súhlasiť.

Otázka v rámci ústnej obhajoby: Aký je aktuálny vývoj v oblasti právnej úpravy kybernetických hrozieb na medzinárodnej a vnútroštátnej úrovni?

Závery:

Hodnotená habilitačnú práca je monotematické dielo, ktoré prináša okrem analýzy existujúcej právnej úpravy kybernetických hrozieb a bezpečnosti aj niektoré nové vedecké postrehy a úvahy *de lege ferenda*. Autor preukázal spôsobilosť samostatne nielen analyzovať, s pomocou zvolených metód a prostriedkov vedeckej práce, aktuálnu, náročnú, zložitú, interdisciplinárnu a mnohorozmernú problematiku, ale aj formulovať príslušné závery.

Habilitačná práca predstavuje prínos do skúmania medzinárodnoprávnych aspektov kybernetických útokov a obohacuje odbornú diskusiu v tejto otázke. Je písaná prehľadne a zrozumiteľne, a preto je privítajú nielen experti na medzinárodné právo, ale aj ďalší odborníci, akademická obec, študenti právnických fakúlt, a tak isto širšia verejnosť, zaujímajúca sa o aktuálne problémy medzinárodného práva a medzinárodných vzťahov.

Habilitant dlhé roky vedecky a pedagogicky pôsobí na Právnickej fakulte UK Bratislava v odbore 3.4.8. medzinárodné právo. Preukázal pedagogickú a odbornú spôsobilosť pôsobiť v rôznych formách výučby a vo všetkých stupňoch a formách štúdia.

Habilitant svojou habilitačnou prácou vytvoril v odbore 3.4.8. medzinárodné právo na Právnickej fakulte UK Bratislava ucelené vedecké dielo, pričom preukázal odborné zvládnutie problematiky ako aj celkový prehľad v otázke medzinárodnoprávnych aspektov kybernetickej bezpečnosti. V odbore 3.4.8. medzinárodné právo na Právnickej fakulte UK Bratislava je v odborných kruhoch uznávanou vedeckou osobnosťou.

Vzhľadom na uvedené, odporúčam habilitantovi po úspešnej obhajobe habilitačnej práce a úspešnom skončení habilitačného konania udeliť vedecký a pedagogický titul „docent“ v odbore 3.4.8. medzinárodné právo.

Doc. JUDr. Peter Vršanský, CSc.

katedra medzinárodného práva a medzinárodných vzťahov
Univerzita Komenského v Bratislave, Právnická fakulta |
peter.vrsansky@flaw.uniba.sk