aut. Szymon Palczewski 26.08.2020

POLSKA POWINNA „WYJŚĆ Z CIENIA” W DEBACIE NAD CYBERBEZPIECZEŃSTWEM [WYWIAD]

„Możemy – jako Polska – wyjść z własną propozycją, z własnym pomysłem na cyberbezpieczeństwo i dzięki temu budować dyskusję w ramach Unii Europejskiej oraz społeczności międzynarodowej” – podkreślił dr Przemysław Roguski, wykładowca prawa międzynarodowego na Uniwersytecie Jagiellońskim. Ekspert w rozmowie odniósł się również do kwestii wyzwań dotyczących prawnego uregulowania cyberprzestrzeni, a także obecnej rywalizacji mocarstw w ramach wirtualnej domeny.

Cyberprzestrzeń jest domeną, która w pełni została stworzona przez człowieka. Jednak pomimo tego powstaje problem związany z prawnym uregulowaniem wirtualnej rzeczywistości, która obejmuje kolejne dziedziny ludzkiego życia oraz funkcjonowania państwa. Zjawisko to jest szczególnie widoczne na poziomie międzynarodowym. Skąd wynika wspomniana trudność? Jakie jest największe wyzwanie dla prawnego uregulowania cyberprzestrzeni?

Trudność wynika przede wszystkim z nowego charakteru cyberprzestrzeni i jej transgraniczności. Od początku lat 90. w części społeczności internetowej panowało przekonanie, że w związku z tym, iż jest to nowoczesna domena, która przekracza granice, nie podlega ona regulacji państwowej. Uważano, że stanowi ona zupełnie inną przestrzeń, wolną od wpływu rządów narodowych. Oczywiście to już wtedy było wątpliwe. Obecnie państwa stosują swoje prawo do wszystkiego, co dzieje się w cyberprzestrzeni. Taki stan rzeczy potwierdzono niejednokrotnie w ramach społeczności międzynarodowej.

Niemniej jednak nadal można zauważyć sytuację, gdzie nadal pokutuje pewne przekonanie dotyczące nowego charakteru cyberprzestrzeni, którą pozornie trudno uregulować. Nawet niektórzy eksperci na łamach ONZ mają wątpliwości odnoszące się do tego, co powinno podlegać przepisom prawa, a co nie. Padają również pytania czy obowiązujące regulacje międzynarodowe są wystarczające dla cyberprzestrzeni, a może jednak należy opracować nowy zestaw norm ze względu na fakt, że mamy do czynienia z wirtualną domeną.

Na te wątpliwości została udzielona odpowiedź w 2015 roku, kiedy to grupa robocza ONZ stwierdziła, że obowiązujące przepisy prawa międzynarodowego mają w pełni zastosowanie do wirtualnej rzeczywistości. Jednak pomimo to, nieustannie pojawia się niepewność wśród dyplomatów.

Czyli podstawowym wyzwaniem dla prawnego uregulowania cyberprzestrzeni jest pozbycie się niepewności?

Tak, z tym że pojęcie „niepewności” jest w tym przypadku wielobiegunowe. Po pierwsze, jak już wspomniałem konsensus, że prawo międzynarodowe ma zastosowanie w cyberprzestrzeni, został osiągnięty, jednak wiedza o nim musi zostać rozpowszechniona nie tylko wśród prawników, ale też osób zajmujących się szeroko rozumianym cyberbezpieczeństwem, zwłaszcza w sferze politycznej i

społeczności technologicznej. To tam właśnie jeszcze możemy zaobserwować gdzieniegdzie „cyberanarchizm". Często pojawiają się głosy, że „państwa nie będą nam mówić, co nam wolno, a czego nie".

Drugi problem dotyczy konkretnego zagadnienia – jak zastosować normy prawne do wyzwań związanych z cyberprzestrzenią. Mamy na przykład powszechny zakaz użycia siły, lecz co to konkretnie oznacza w kontekście wirtualnej domeny? Tutaj pozostaje nam pole do popisu i aktywnej dyskusji. Musimy znaleźć konsensus co do interpretacji poszczególnych pojęć.

Każdy kraj posiada własne podejście do działalności w cyberprzestrzeni. Państwa różnią się również sposobem tworzenia oraz interpretowania przepisów prawa. Te rozbieżności są zauważalne przede wszystkim na poziomie międzynarodowym, co odzwierciedlają między innymi dyplomatyczne spory. W związku z tym, jakie państwa są obecnie najbardziej otwarte na współpracę w zakresie stworzenia kompleksowego zestawu norm dotyczących cyberprzestrzeni na poziomie międzynarodowym, a które z nich są wręcz przeciwne tego typu inicjatywom?

Na samym początku należy podkreślić, że na płaszczyźnie ONZ funkcjonują dwa zespoły, które zajmują się kwestią stosowania prawa międzynarodowego w cyberprzestrzeni. Jednym z nich jest zespół ekspertów rządowych (Group of Governmental Experts, GGE) odpowiedzialny między innymi za interpretację prawa międzynarodowego. Po drugie, istnieje alternatywny projekt – otwarta grupa robocza (Open-Ended Working Group, OEWG). Nie zamyka się ona na żadne państwo, a w jej ramach trwają negocjacje na temat opracowania skutecznych norm dotyczących cyberprzestrzeni.

W związku z tym w odpowiedzi na powyższe pytanie możemy zauważyć trzy kwestie. Po pierwsze, obowiązuje konsensus z 2015 roku, mówiący o tym, że prawo międzynarodowe ma zastosowanie w cyberprzestrzeni oraz że istnieją tzw. „cybernormy". Wspomniane porozumienie jest jednak podważane przez grupę państw zdominowanych przez Rosję i Chiny oraz ich sojuszników, które uważają, że w prawdzie regulacje te mają zastosowanie, ale nie w pełnym zakresie. Moskwa, a także Pekin chciałyby, aby normy prawa obowiązywały wybiórczo. To znaczy, opowiadają się za uregulowaniem korzystnych dla ich rządów aspektów prawa, takich jak poszanowanie suwerenności czy nie mieszanie się w sprawy wewnętrzne. Natomiast pozostałe dziedziny, na przykład prawa człowieka oraz odpowiedzialność międzynarodowa, schodzą na dalszy plan. Co więcej, szokujący jest fakt, że w lutym bieżącego roku Chiny stwierdziły, iż w ogóle zasady o odpowiedzialności międzynarodowej nie są jeszcze ugruntowane w prawie międzynarodowym. Oczywiście jest to kompletna bzdura…

Z drugiej strony mamy państwa – nazwijmy je – „Zachodnie". Starają się one zbudować koalicję, która stworzy porozumienie oparte na stosowaniu przewidywalnych zasad prawnych. Do tej grupy zaliczamy Stany Zjednoczone, państwa Unii Europejskiej, Australię, Singapur. Japonia jest również bardzo aktywna w tym zakresie. Są to generalnie demokracje typu zachodniego, które chcą, żeby „reguły gry były jasne".

Trzecią grupę stanowią państwa „po środku", które się jeszcze nie określiły, ale będą musiały to prędzej czy później zrobić. Wśród nich można wymienić między innymi Indie. Przez długi czas New Delhi milczało, jednak w związku z trwającymi napięciami z Chinami zaczyna powoli definiować swoją politykę w zakresie prawnego uregulowania cyberbezpieczeństwa. Zobaczymy, co z tego wyjdzie.

Czy uważa Pan, że państwa Zachodu oraz kraje grupy rosyjsko-chińskiej są w stanie w jakiś sposób się porozumieć i doprowadzić do konsensusu w sprawie opracowania jednolitych, wspólnych norm? Czy jest to sytuacja zupełnie niemożliwa?

Obecnie jest to bardzo trudne. Przejawem tego jest fakt, że nawet grupa ekspertów rządowych ONZ w swoim mandacie porzuciła poszukiwanie konsensusu. Efekt prac GGE, które zakończą się w najbliższym czasie, stanowić ma raport, jednak nie będzie miał on charakteru konsensualnego. Warto jednak podkreślić, że każde państwo zostało zobligowane do załączenia do opracowanego dokumentu swoją interpretację stosowania norm prawnych w cyberprzestrzeni. W związku z tym widzimy, że już na tym poziomie zachodzi pewien „zgrzyt".

Równocześnie trzeba zaznaczyć, że istnieją pewne pola do kompromisu czy też zbliżenia. Są prowadzone dyskusje na temat tego czy na przykład w ogóle jest potrzebny jakiś nowy traktat międzynarodowy regulujący kwestie cyberprzestrzeni. Państwa Zachodnie obecnie mówią „nie" dla stworzenia nowego, kompleksowego dokumentu. Z kolei wśród doradców, prawników czy polityków pojawiają się twierdzenia, że traktat miałby sens, gdyby nie podważał tego, co już ma zastosowanie.

Główny problem polega na tym, że występuje tutaj brak zaufania. Mówiąc prościej, jedna strona nie ufa drugiej, wskazując, że nie będzie ona grała rzetelnie. Zachód uważa, że Wschód działa na czas bądź też „rzuca kłody pod nogi", aby więcej problematycznych kwestii pozostało w ukryciu.

Możemy więc powiedzieć, że wkracza nam tutaj teoria realizmu.

Tak, tylko przy czym należy zauważyć, że nie jest w cale tak, iż państwa zachodnie są blokiem monolitycznym. Tutaj też są dość znaczne różnice w interpretacji. Na przykład istnieje problem czy zasada suwerenności jest konkretną normą prawną czy tylko ogólną zasadą, i co z tego wynika. W tym kontekście Stany Zjednoczone oraz Wielka Brytania mają wspólne zdanie – Francja, Holandia, Niemcy czy też ostatnio Czechy odrębne. A istnieje jeszcze wiele państw będących pośrodku, w tym między innymi Polska.

Warto podkreślić, że my jako Rzeczpospolita wyrażamy poparcie dla postanowień wypracowanego konsensusu, iż prawo międzynarodowe ma zastosowanie w cyberprzestrzeni, ale własnego programu, czy też wizji jak należy to wszystko interpretować, do tej pory nie przedstawiliśmy. W związku z tym widzimy, że jest tutaj dużo do zrobienia nawet w ramach samej Unii Europejskiej, a co dopiero między zwaśnionymi blokami – Wschodnim i Zachodnim.

Kolejnym problemem dotyczącym prawa i cyberprzestrzeni jest „rozbieżność w czasie". Powstawanie kolejnych zagrożeń w wirtualnej rzeczywistości wiąże się z szybko postępującym rozwojem technologicznym. Z kolei tworzenie prawa jest zjawiskiem, które wymaga upływu określonego przedziału czasu. Czy w jakikolwiek sposób można wyeliminować tę problematyczną rozbieżność? I czy prawo w jakimś stopniu może przewidzieć wspomniane zmiany i zagrożenia?

Oczywiście taki problem istnieje, ponieważ tworzenie prawa, zwłaszcza na płaszczyźnie międzynarodowej, jest żmudnym procesem. W tym miejscu należy wskazać na dwa podstawowe źródła prawa międzynarodowego. Pierwsze stanowią traktaty, czyli umowy międzynarodowe, na które państwa muszą się zgodzić. Ich tworzenie wiąże się z długim procesem negocjacji, później ratyfikacji… To wszystko trwa.

Drugim źródłem jest zwyczaj międzynarodowy, który powstaje w oparciu o praktykę państw oraz przekonanie, że praktyka odpowiada zobowiązaniom prawnym.

Obecnie jedynym traktatem, który reguluje kwestie cyberbezpieczeństwa w szerokim rozumieniu tego słowa jest konwencja budapesztańska o cyberprzestępczości z 2000 roku. Jej opracowanie było długim i żmudnym procesem. Od pewnego czasu istnieje również chęć stworzenia protokołu dodatkowego.

Co warte podkreślenia, Rosja na łamach ONZ zaproponowała zupełnie nową konwencję ze względu na

fakt, że Moskwie „niezbyt się podobają” zapisy obowiązującego traktatu. Kreml silnie lobbuje w tej sprawie, ale, ogólnie rzecz biorąc, opracowanie nowej, powszechnej regulacji jest obecnie bardzo trudne.

Z drugiej strony zwyczaj międzynarodowy też nie powstaje od razu. Wymaga pewnej ustalonej praktyki państw i to nie jednego czy dwóch, ale większej liczby, w oparciu o przekonanie prawne, którego nam obecnie brakuje.

Ponieważ tworzenie nowego prawa – czy to traktatowego, czy zwyczajowego – jest czasochłonne, obecnie tym, co najszybciej może zadziałać z punktu widzenia norm międzynarodowych, nie jest tworzenie nowych regulacji, lecz tzw. dynamiczna czy też ewolucyjna interpretacja przepisów już istniejących. Każde państwo może przedstawić swoją wykładnię stosowania pewnych norm w cyberprzestrzeni, na bazie czego wyciąga się ogólne wnioski, które z kolei rozwijają katalog możliwości interpretacji danej normy w odniesieniu do konkretnej sytuacji.

Państwa rywalizują ze sobą w cyberprzestrzeni i jest to niezaprzeczalny fakt. Bardzo często rządy realizują agresywne kampanie, w tym operacje hakerskie czy dezinformacyjne, aby osiągnąć swoje cele polityczne, ekonomiczne, społeczne itd. W związku z tym pojawia się pytanie – jak wygląda odpowiedzialność państw za prowadzenie złośliwych działań w stosunku do innego kraju w sieci? Czy na przykład Rosja może zostać objęta sankcjami za operacje informacyjne wymierzone w amerykańskie wybory z 2016 roku?

Prawo międzynarodowe wymaga w zakresie odpowiedzialności międzynarodowej dwóch rzeczy. Po pierwsze, naruszenia zobowiązania międzynarodowego, czyli musimy stwierdzić czy istnieje jakaś norma, która została naruszona. W przypadku ingerencji w wybory najczęściej mówi się o zasadzie nieinterwencji, czyli zakazie interwencji w sprawy wewnętrzne państwa. Wynika to z faktu, że ustalenie własnego systemu politycznego należy do trzonu kompetencji państwa, tzw. *domaine réservé*, objętych jego wyłączną jurysdykcją.

Drugim elementem jest przypisanie danego działania państwu, a więc niezbędne jest udowodnienie, że konkretny czyn został przeprowadzony przez organy państwa lub też przez podmioty, które znajdują się pod ich kontrolą. We wspomnianym wyżej wątku chodzi o aktorów rosyjskich.

W momencie, gdy wszystkie warunki zostaną spełnione możliwe jest wyciąganie konsekwencji między innymi w postaci środków odwetowych. Przykładowo, jeżeli jedno państwo atakuje drugie za pomocą ataku hakerskiego, drugie może odpowiedzieć tym samym, aby ten atak hakerski zatrzymać.

Sprawa staje się zdecydowanie bardziej skomplikowana w kontekście kampanii dezinformacyjnych, ponieważ powstaje tutaj problem kwalifikacji prawnej – czy rozpowszechnianie fake newsów stanowi już naruszenie zakazu nieinterwencji w sprawy wewnętrzne? Obecnie nie jest to do końca jasne. Na ten moment pojęcie „interwencji w sprawy wewnętrzne” odnosi się do *domaine réservé*, czyli obszaru wyłącznej kompetencji państwa i wiąże się z zastosowaniem środku przymusu. Pojawia się tutaj kluczowe pytanie: czy puszczanie fałszywych informacji to jest już przymuszenie państwa do „czegoś więcej”?

Obecnie państwa są zgodne co do tego, że gdyby nastąpiła bezpośrednia manipulacja wynikami wyborów; gdyby komputery, które są używane do zdalnego liczenia głosów; albo infrastruktura przeznaczona do przeprowadzenia procesu wyborczego została zainfekowana jakimś złośliwym oprogramowaniem, wówczas stanowi to naruszenie prawa międzynarodowego i istnieje możliwość odpowiedzi.

W innych przypadkach nie ma pełnej zgodności i w związku z tym występuje pewien problem odnoszący się do odwetu z punktu widzenia prawa. Przy czym należy pamiętać, że zawsze można nałożyć sankcje, które nie zaliczają się do kategorii środków odwetowych.

Konieczne jest podkreślenie, że „środki odwetowe" potrzebują uzasadnienia tylko wtedy, jeśli same naruszają prawo międzynarodowe. Z kolei sankcje, czyli na przykład zakaz wjazdu na terytorium danego państwa dla konkretnych osób albo zamrożenie jakichś aktywów finansowych, nie naruszają bezpośrednio zobowiązań międzypaństwowych, a przez to są zdecydowanie łatwiejszym środkiem do uruchomienia.

Wspomniał Pan, że tego typu działania muszą zostać przypisane konkretnemu państwu, czyli w tym wypadku Rosji. Kto w takim razie może przypisać dane działanie innemu państwu? Czy właściwe w tym wypadku są służby i organy poszkodowanego kraju czy może jakieś zewnętrzne agencje?

Przypisuje zawsze ten kraj, który powołuje się na czyn międzynarodowo bezprawny, aby w ten sposób pociągnąć do odpowiedzialności państwo, działające we wrogich intencjach. Czyli jeżeli Stany Zjednoczone padły ofiarą operacji zabronionej przez prawo międzynarodowe, mogą przypisać ten czyn Rosji i wprowadzić narzędzia odwetowe.

Nie ma jednak centralnego organu przypisującego odpowiedzialność. Natomiast należy mieć na uwadze, że oczywiście każde państwo ponosi ryzyko, iż gdy wspomniane wcześniej przypisanie okaże się niesłuszne, ze względu na przykład na złe informacje wywiadowcze albo wadliwość dowodów, w momencie powstania sporu międzynarodowego autor oskarżenia sam ponosi odpowiedzialność międzynarodową. W przypadku „pomyłki" państwo nie ma prawa reagować w stosunku do drugiego.

Czy taka sytuacja nie rodzi kolejnego problemu dotyczącego braku obiektywizmu związanego z przypisaniem danego działania innemu państwu, zwłaszcza gdy głównym podejrzanym jest jeden z przeciwników? Wiele faktów może być „naciąganych", aby w jakikolwiek sposób wykazać winę adwersarza.

Nie zgodziłbym się z tak śmiałą tezą, ponieważ państwa bardzo rzadko dokonują otwartego, publicznego przypisania wrogich działań innemu państwu z racji tego, że nie chcą się wiązać konsekwencjami, nawet w sposób polityczny.

Środowisko prawnicze bardzo często wręcz ubolewa nad tym, że pewne działania hakerskie powodują znikome reakcje ze strony państw. Mówi się, że nastąpił atak ze strony aktora państwowego, a nie wskazuje na żadne konkrety. Nie przedstawia się dowodów lub innych informacji, na jakiej podstawie dane stwierdzenie padło.

Obecnie mamy raczej sytuację, gdzie te przypisania nie są aż takie liczne, a nawet jeśli następują, to państwa nie podają podstaw prawnych czy też innych danych, na bazie których dokonano tego przypisania.

Reakcje zbrojne na cyberataki są już przewidywane w strategiach państw. Na przykład Stany Zjednoczone zastrzegają sobie prawo do reakcji na tego typu zagrożenia wszelkimi koniecznymi i odpowiednimi środkami. W polskim ustawodawstwie ataki w cyberprzestrzeni zostały potraktowane na równi ze zbrojną napaścią na terytorium Rzeczpospolitej Polskiej czy atakami terrorystycznymi jako zagrożenie zewnętrzne państwa uzasadniające wprowadzenie stanu wojennego. Czy tego typu działania pozostają w zgodzie z prawem międzynarodowym? W jakich przypadkach mogą mieć zastosowanie?

Tak, przy czym musimy oddzielić sferę ustawodawstwa krajowego i działań na płaszczyźnie

wewnętrznej od reakcji prawnomiędzynarodowych. W prawie międzynarodowym bardzo ważne jest stopniowanie pewnych reakcji. To znaczy, że w momencie kiedy nastąpi naruszenie prawa międzynarodowego przez stronę drugą, wtedy możemy podjąć środki odwetowe. Jednak nigdy nie mogą być one środkami siłowymi. Mówiąc prościej, nie wolno użyć siły w odwecie, chyba że w odpowiedzi na napaść zbrojną. Natomiast, jeśli to nie jest napaść zbrojna, należy użyć środków pokojowych. Oczywiście muszą być one proporcjonalne, niezbędne, konieczne i tak dalej. Tutaj nie ma ograniczeń i de facto można ich użyć. Warto również dodać, że dopuszczalna jest odpowiedź na przykład poprzez nakładanie sankcji handlowych.

W odniesieniu do możliwych środków odpowiedzi na cyberataki, ostatnio Unia Europejska nałożyła sankcje na sześć osób i trzy podmioty odpowiedzialne za różne kampanie hakerskie, w tym cyberatak na Organizację ds. Zakazu Broni Chemicznej (OPCW). Działania ze strony Wspólnoty należy rozpatrywać w kategoriach „kroku milowego" w budowie cyberbezpieczeństwa? A może jest to jedynie sukces dyplomatyczny, który w rzeczywistości nie powstrzyma hakerów?

No cóż, kwestia skuteczności sankcji czy to europejskich czy amerykańskich jest jeszcze przedmiotem badań jakościowych i ilościowych w tym zakresie. Obecnie czekamy na ich wyniki. Amerykanie jednak uważają, że podjęte przez nich kroki – nie tylko sankcje, ale też bardziej aktywne działania – doprowadziły do zaprzestania konkretnych prób cyberataków, na przykład ze strony Rosji, których celem były *midterm elections*.

Odnosząc się do samych sankcji przeciwko wybranym podmiotom i osobom, należy podkreślić, że nie dotyczą one państw, lecz konkretnych jednostek. Na ile są skuteczne…? Na pewno są ważne z dwóch powodów, przynajmniej w przypadku europejskim. Po pierwsze, sam fakt, że Unia Europejska zauważyła, że cyberataki stanowią problem i stworzyła arsenał pewnych środków dyplomatycznych, z których następnie zdecydowała się z korzystać. I to już samo w sobie jest dużym sukcesem, bardzo ważnym krokiem naprzód. Obecnie są już prowadzone rozmowy na temat objęcia restrykcjami kolejnych podmiotów. Mowa tu o osobach odpowiedzialnych za atak na niemiecki parlament. Ważne jest, żeby Unia Europejska podtrzymywała to, co samodzielnie wypracowała, ponieważ stanowi to również sygnał dla zewnętrznych podmiotów, że pewne zachowania nie będą akceptowane.

Powstaje natomiast pytanie co dalej? Czy się zatrzymamy na tym etapie? A może będzie to jeszcze częściej stosowane rozwiązanie i zdecydowanie szybciej? Zauważmy, że te sankcje, które zostały teraz wprowadzone odnoszą się do ataków hakerskich, jakie miały miejsce dwa lata temu i nie objęły wszystkich aktorów.

W tym miejscu należy również dodać, że sankcje w praktyce niektórych państw stały się standardowym narzędziem odpowiedzi na złośliwe działania w cyberprzestrzeni. Ale czy to samo w sobie powstrzyma hakerów? Zobaczymy. Być może podjęcie bardziej aktywnych działań stanie się koniecznością.

Cyberprzestrzeń to jednak nie tylko państwa. Wirtualna rzeczywistość stanowi również domenę funkcjonowania niezależnych ugrupowań hakerskich lub indywidualnych cyberprzestępców, którzy realizują swoje zadania z różnych pobudek. Jak wygląda kwestia kwalifikacji złowrogich czynów w cyberprzestrzeni z perspektywy prawa? Czy na przykład kradzież danych można objąć kodeksową definicją kradzieży?

Tutaj musimy odróżnić sferę prawa wewnętrznego danego państwa od kwestii regulacji międzynarodowych. W normach krajowych takie czynności jak naruszenie poufności danych czy integralności systemów komputerowych są objęte sankcjami karnymi – o tym mówiła już konwencja budapesztańska. Istnieją również odpowiednie przepisy unijne i, zgodnie z zasadami UE, Polska

implementowała je do kodeksu karnego. W związku z tym możemy stwierdzić, że na przykład włamanie się do komputera w celu kradzieży danych stanowi przestępstwo, które jest objęte karą.

Natomiast ciekawsza jest kwestia jak to wygląda na poziomie międzynarodowym. Wszystko tutaj zależy od tego, czy haker wykazuje związek z jakimś państwem. Jeśli za dany czyn odpowiada cyberprzestępca działający indywidualnie bądź też w ramach jakiejś grupy – wtedy jest to tylko kwestia prawa karnego. Natomiast gdy pracuje na zlecenie jakiegoś organu państwowego, na przykład jednostki wojskowej lub wywiadowczej, bądź też działa pod kontrolą rządu, wówczas jego działanie można przypisać państwu i w takiej sytuacji również ono ponosi odpowiedzialność międzynarodową.

Bardzo interesująca jest sprawa związana z kradzieżą danych. Istnieje duży spór czy wspomniany czyn w ogóle narusza zobowiązania międzynarodowe. Eksperci ze Stanów Zjednoczonych i Wielkiej Brytanii uważają, że nie. Każdy może sobie odpowiedzieć dlaczego tak jest… Kto ma duży potencjał wywiadowczy i kto ten swój potencjał chce chronić… Ale jako prawnik muszę zaznaczyć, że nie czyni to naszej argumentacji łatwiejszej, ponieważ jeżeli sami uważamy, że kradzież informacji nie jest naruszeniem żadnych norm międzynarodowych, to dlaczego się oburzamy, że Rosja czy Chiny podejmują podobne działania?

Przechodząc na krajowe podwórko, widzimy, że Polska rozwija Wojska Obrony Cyberprzestrzeni. Nic jednak nie wiadomo na temat ich podejścia do prawnego aspektu działań w sieci. Jak to wygląda w innych państwach i czy takie podejście powinno być spisane?

Oczywiście kwestia ta musi być uregulowana, ponieważ podobne jednostki w żadnym państwie nie działają w próżni prawnej. Co więcej, funkcjonują jako organ państwa w przypadku podjęcia operacji w obcych sieciach. Warto jednak wyjaśnić, że w momencie, gdy działają tylko w ramach obrony krajowych sieci informatycznych i w ramach państwowej infrastruktury, posiadają autoryzację na podstawie prawa krajowego. Ale w sytuacji, kiedy przeprowadzałyby akcję poza granicami państwa w obcych sieciach, muszą mieć uzasadnienie i podstawę prawną na gruncie norm międzynarodowych. W związku z tym konieczne jest opracowanie klarownej regulacji prawnej, żeby żołnierz Wojsk Obrony Cyberprzestrzeni nie zastanawiał się co mu wolno a czego nie – musi mieć jasne wytyczne. To dotyczy zarówno wszelkich operacji prowadzonych w czasie pokoju, jak i operacji prowadzonych w ramach konfliktu zbrojnego. W przeciwnym wypadku istnieje realne ryzyko, że podjęcie określonych działań może naruszyć prawo międzynarodowe, a to – jak już wiemy – prowadzi do odpowiedzialności międzynarodowej państwa jako całości.

W innych krajach obowiązują różne dyrektywy i wytyczne dotyczące działań w cyberprzestrzeni. W odniesieniu do Polski, słuszne wydaje się rozpoczęcie całej procedury od zastanowienia się jak Rzeczpospolita w ogóle interpretuje normy prawa międzynarodowego w cyberprzestrzeni. Można się tutaj posłużyć na przykład rozwiązaniami amerykańskimi czy dokumentami francuskimi. Francuzi przeprowadzili fantastyczną analizę, mają bardzo dużo świetnych dokumentów pod kątem zarówno interpretacji prawa, jak i też dostosowania norm prawa wewnętrznego do funkcjonowania cyberwojsk. Można więc popatrzeć na to, co robią sojusznicy oraz stworzyć taką podstawę, która wskazywałaby jasne zasady działania zarówno naszym żołnierzom, jak i innym państwom, w tym również naszym adwersarzom, w celu wyjaśnienia naszej strategii w wirtualnej domenie – w jaki sposób będziemy reagować, gdzie i na jakiej podstawie. Czyni to nasze działania przewidywalnymi, wpływa na rozwój prawa międzynarodowego i ogólnie wzmacnia stabilność w stosunkach międzynarodowych.

Czyli najlepszym rozwiązaniem będzie czerpanie z doświadczenia innych?

Absolutnie tak, nie ma potrzeby „wymyślać koła na nowo”. Co więcej, gdybyśmy się włączyli jako

Polska do dyskusji, która jest prowadzona na poziomie międzynarodowym, to moglibyśmy realnie wpływać na kształt tej debaty. A zauważmy, że w kwestii interpretacji prawa międzynarodowego takie swoje poglądy przedstawiły między innymi Stany Zjednoczone, Wielka Brytania, Francja, Niderlandy, Estonia, Niemcy czy Czechy. Jak widać, wiele państw Unii Europejskiej jeszcze czegoś takiego nie zrobiło, więc tutaj możemy – jako Polska – wyjść z własną propozycją, z własnym pomysłem na cyberbezpieczeństwo i dzięki temu budować dyskusję w ramach Unii oraz społeczności międzynarodowej. W ten sposób będziemy posiadali możliwość realnego wpływu na kształt tej dyskusji. Im wcześniej Polska zaangażuje się w coś takiego w sposób przemyślany i profesjonalny, tym większy wkład może mieć w kształtowanie rzeczywistości, a nie tylko być biernym odbiorcą norm ustalonych już wcześniej przez innych.

Czytaj też: Gen. Gromadziński: W wojsku musimy być świadomymi użytkownikami sieci - od szeregowego po generała