aut. Andrzej Kozłowski 15.03.2018

PATRYK PAWLAK: CYBERBEZPIECZEŃSTWO TO INWESTYCJA, KTÓRA SIĘ ZWRÓCI [WYWIAD]

O prawie międzynarodowym w cyberprzestrzeni, budowaniu zdolności cybernetycznych innych państw oraz szansie dla Polski mówi w rozmowie z CyberDefence24.pl doktor Patryk Pawlak z Instytutu Unii Europejskiej Studiów nad Bezpieczeństwem.

CyberDefence24.pl: Jak w Brukseli, na poziomie Unii Europejskiej oceniany jest pomysł Cyfrowej Konwencji Genewskiej?

dr Patryk Pawlak: Propozycja Cyfrowej Konwencji Genewskiej przedstawiona przez firmę Microsoft nie jest przyjęta zbyt pozytywnie w Brukseli. Wynika to przede wszystkim z tego, że jest ona sprzeczna z podejściem które Unia Europejska forsowała w ciągu kilku ostatnich lat. Wystarczy przeanalizować konkluzje Rady Europejskiej odnośnie cyberdyplomacji czy Komunikat przedstawiony w 2017 roku o odporności, prewencji i obronie w cyberprzestrzeni. W obu dokumentach Unia Europejska konsekwentnie powtarza, że istniejące prawo międzynarodowe, łącznie z całością Konwencji Narodów Zjednoczonych, obowiązuje również w cyberprzestrzeni. To jest też wniosek przedstawiony w 2015 roku przez grupę ekspertów rządowych [*Group of Governmental Experts*, GGE – przyp. red.] przy ONZ. I tego argumentu trzyma się Unia Europejska jeżeli chodzi o jakiekolwiek propozycje nowych międzynarodowych aktów prawnych. Jednym z problemów – abstrahując od kwestii czy byłoby to możliwe ze względów czysto logistycznych, bo pamiętajmy, że przyjmowanie konwencji trwa latami, jeżeli nie dziesięcioleciami – jest to, że pomysły nowych konwencji pojawiały się również ze strony innych krajów, takich jak Chiny czy Rosja. Szanghajska Organizacja Współpracy, w której Chiny i Rosja odgrywają główną rolę, zaproponowała swoje rozwiązanie w formie „kodeksu postępowania" znacznie wcześniej i było one konsekwentnie krytykowane [*Code of conduct*– przyp. red.]".

Który miałby być zbieżny z Cyfrową Konwencją Genewską?

To nie jest zbieżność jeśli chodzi o samą zawartość tych propozycji. Jednak główne pytanie, które prowadzi nasze rozumowanie oraz pytanie, które wszyscy sobie zadają, tj. czy obowiązujące prawo międzynarodowe ma zastosowanie w cyberprzestrzeni czy nie. Odpowiedź na to pytanie została podana przez kilka różnych organizacji. W ramach tzw. procesu tallińskiego i opublikowanych podręczników grupa ekspertów od prawa międzynarodowego oceniła, że prawo międzynarodowe ma zastosowanie i podała szerokie uzasadnienie. Raporty opublikowane przez Grupę Ekspercką przy ONZ w 2013 i 2015 roku stwierdziły dokładnie to samo. Pomimo tego, że żaden z tych dokumentów nie ma mocy prawnej, ich wnioski kształtują myślenie krajów członkowskich Unii Europejskiej. Więc jakikolwiek pomysł nowej konwencji jest sprzeczny z tą linią argumentów.

Pomysł nowej konwencji nie jest jedynie pomysłem Microsoftu. Podobne idee pojawiały się też jeżeli chodzi o walkę z cyberprzestępczością. Przedstawia ją najczęściej strona rosyjska i chińska. To wpisuje się w pewną szerszą dyskusję na temat tego czy nowe konwencje są potrzebne czy nie.

Jak omawiamy kwestie Konwencji to warto wrócić do Konwencji Budapesztańskiej z 2001 roku dotyczącej walki z cyberprzestępczością.

Dlatego też nie potrzebujemy nowej konwencji ds. walki z cyberprzestępczością, ponieważ mamy już taki dokument. Konwencja Budapesztańska stała się pewnym standardem.

Czy ona faktycznie ma jakieś znaczenie, ponieważ jest oceniana krytycznie przez ekspertów, chociażby ze względu na to, że nie przystąpiły do niej Rosja czy Chiny i zakres jej stosowania jest dość mały. Jak Pan ją ocenia?

Chcemy mieć pewien standard i moim zdaniem, funkcję tę pełni właśnie Konwencja Budapesztańska. To obecnie jest jedyny dokument na świecie, który określa ramy współpracy międzynarodowej jeżeli chodzi o walkę z cyberprzestępczością. Nie ma innego dokumentu, który by w jakiś sposób tym się zajmował. Istnieje na przykład Konwencja Unii Afrykańskiej o Cyberbezpieczeństwie i Ochronie Danych Osobowych z 2014 roku, ale zawiera ona wiele postanowień sprzecznych z podejściem promowanym przez UE. Konwencja Budapesztańska jest jedynym dokumentem, który nie tylko dotyczy walki z cyberprzestępczością, ale wpisuje się w szerszy porządek prawny dotyczący, na przykład, ochrony praw człowieka. Tego elementu brakuje w innych porządkach prawnych, włącznie z tym w ramach Unii Afrykańskiej. Nie możemy wspierać walki z cyberprzestępczością i budować silnych oddziałów policji, nie przywiązując jednocześnie uwagi do tego czy system prawny w danym kraju również gwarantuje pewne swobody obywatelskie, bo to bardzo łatwo mogłoby doprowadzić do sytuacji, gdzie całe wsparcie, którego dostarczamy miejscowym oddziałom policji, jest jednocześnie wykorzystywane do prześladowania obrońców praw człowieka czy organizacji pozarządowych.

Dlaczego Rosja czy Chiny nie przystąpiły do Konwencji Budapesztańskiej? Jakich argumentów używano?

To nie tylko Rosja, Chiny, ale też np. Indie. Wiele z tych argumentów ma charakter ideologiczny. Ta konwencja jest postrzegana jako konwencja Zachodu i to jest główny powód sprzeciwu wobec niej. Część krytyki skupia się również na wysokim standardzie prawnym proponowanym przez Konwencję Budapesztańską, które nie zawsze są łatwe do wprowadzenia. Jednak należy mieć na uwadze to, że promowanie rozwiązań zawartych w Konwencji Budapesztańskiej nie skupia się tylko na tym, by zachęcić inne kraje do jej przyjęcia. Wsparcie, dostarczane przez Unię we współpracy z Radą Europy w ramach programów budowy zdolności do walki z cyberprzestępczością skupia się na tak naprawdę na zbliżaniu systemów i rozwiązań prawnych do tego, co proponuje Konwencja. Podejście do Konwencji jest zatem mniej dogmatyczne niż zazwyczaj się podaje.

Praktycznym dowodem tej zmiany w podejściu jest np. sposób dystrybuowania środków na budowanie zdolności cybernetycznych. Parę lat temu, programy, które były zarządzane przez Radę Europy i dotyczyły walki z cyberprzestępczością miały jako jeden z warunków otrzymania środków przystąpienie do Konwencji Budapesztańskiej. W najnowszych programach takich jak GLACY+ tego warunku już nie ma. Zamiast tego celem jest jak najobszerniejsze zbliżenie rozwiązań prawnych obowiązujących w danym kraju, z tymi proponowanymi przez Konwencję Budapesztańską. Rada Europy dyskutuje obecnie możliwości nowych protokołów, które ułatwiłyby współpracę z innymi krajami. Należy jednak jeszcze raz podkreślić, że na dzień dzisiejszy Konwencja Budapesztańska to jedyny dokument międzynarodowy zawierający konkretne rozwiązania prawne, które pomagają państwom, między innymi, jeśli chodzi o zabezpieczenie oraz wymianę elektronicznych materiałów dowodowych.

Jak Pana Instytut wspiera Unię Europejską w działaniach z obszaru cyberbezpieczeństwa?

Są dwie główne linie badań. Głównym obszarem jeśli chodzi o cyberbezpieczeństwo jest wspieranie

projektów dotyczących budowania i wspierania zdolności cybernetycznych poza Unią Europejską. Od 2015 roku Instytut jest zaangażowany w badania mające na celu stworzenie pewnych struktur analitycznych odnośnie ogólnego podejścia do budowania zdolności cybernetycznych oraz wyznaczania priorytetów współpracy z innymi krajami. Głównym problem, który się pojawił, a zarazem główne pytanie, które sobie postawialiśmy jeśli chodzi o badania, było powiązanie budowania zdolności w cyberprzestrzeni z polityką rozwojową. To jest coś, co nie jest jeszcze powszechnie przyjęte pomimo raportów organizacji takich jak Bank Światowy.

Czy one są tylko wspominane w dokumentach? Czy faktycznie coś się dzieje w tym obszarze?

Dzieje się bardzo dużo. Jest dużo projektów, które KE wspiera i prowadzi wspólnie z Radą Europy jeśli chodzi o walkę z cyberprzestępczością. Jest też kilka projektów, które UE prowadzi sama. Od 2014 to 2016 roku francuska organizacja Expertise France realizowała za pieniądze unijne projekt ENCYSEC skupiony na kilku państwach bałkańskich: Kosowie, Mołdawii oraz Macedonii. Obecnie realizowany jest także znacznie większy projekt CYBER4D, którego liderem jest NI-CO z Irlandii Północnej, a w którym udział biorą także Wielka Brytania, Estonia i Holandia. Projekt ten swoim zasięgiem obejmuje Afrykę i Azję. Dla porównania warto podać, że budżet pierwszego to 1,5 miliona euro, a drugiego 11 milionów euro.

Pisał Pan w przeszłości o *soft power* Unii Europejskiej w cyberprzestrzeni. Czy Pana zdaniem budowanie cyber zdolności w krajach trzecich może przysłużyć się realizacji tego pomysłu?

Zdecydowanie. Jest to jeden z głównych instrumentów, które UE tak naprawdę posiada. Finanse, którymi UE dysponuje, nigdy nie będą porównywalne z tym, co ma sektor prywatny jeśli chodzi o cyberbezpieczeństwo i możliwości inwestycji. Natomiast w porównaniu z tym, co inwestują inne kraje, jak USA, to jest to obszar, w którym nie mamy sobie nic do zarzucenia. Jednak powinniśmy wykorzystywać nasze zaangażowanie w sposób bardziej strategiczny. Taka możliwość została dostrzeżona przez instytucje unijne. Propozycje, które zostały przedstawione przez KE w cyber pakiecie z ubiegłego roku, zawierają bardzo konkretne odniesienia do potrzeby budowy nowej sieci organizacji sektora prywatnego oraz instytutów badawczych, które miałby wspierać UE w budowie zdolności cybernetycznych w krajach trzecich. Tam również pojawia się pomysł przyjęcia politycznych wyznaczników jeśli chodzi o budowanie zdolności innych krajów, co tak naprawdę odbieram jako chęć określenia pewnych ram politycznych i zdefiniowaniu priorytetów, kiedy te instrumenty powinny być wykorzystywane.

Jaki wkład może wnieść Polska indywidualnie jako kraj członkowski do wspólnego dorobku obszarze soft power?

Mam nadzieje, że możliwości włączenia się do kształtowania unijnego podejścia w tym zakresie zostaną szybko dostrzeżone przez nasz rząd. Mamy w Polsce wspaniałych informatyków, którzy obecnie wspierają zdolności wielu krajów UE. Posiadamy też dobre zdolności analityczne, jeśli chodzi o analizę zagrożeń. Moim zdaniem jest to potencjalne pole do popisu dla różnych instytucji w Polsce, placówek badawczych, ale też rządu, który w większości innych krajów ponosi główny ciężar zebrania dostępnej ekspertyzy i promowanie jej.

Jakie jest zainteresowanie innych krajów?

Zainteresowanie unijnymi inicjatywami zależy od priorytetów, jakie stawiają sobie poszczególne rządy. Kilka państw jest wyraźnymi liderami jeśli chodzi o kwestie cyberbezpieczeństwa i budowania zdolności w tym zakresie. Francja, Wielka Brytania, czy Holandia są zainteresowane budowaniem

zdolności cybernetycznych w krajach trzecich. Z kolei Portugalia jest jednym z krajów realizujących unijne projekty dotyczące cyber obronności. Jak dotychczas udział Polski w tych inicjatywach jest ograniczony. A pole do popisu jest, bo nowe inicjatywy i projekty są regularnie ogłaszane i publikowane. Ale by w pełni zrealizować drzemiący w Polsce potencjał potrzebna jest przede wszystkim wola polityczna oraz zaangażowanie konkretnych środków na wsparcie polskich struktur badawczych. Cyber pakiet przedstawiony przez Komisję jesienią 2017 roku przewiduje szereg konkretnych kroków, w których realizacji Polska mogłaby uczestniczyć. Dotyczy to między innymi Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego czy stworzenia unijnej sieci instytucji wspierających budowanie zdolności cybernetycznych: ESDZ, organy państw członkowskich odpowiedzialne za bezpieczeństwo cybernetyczne, agencje UE, służby Komisji, środowisko akademickie i społeczeństwo obywatelskie. Z racji tego, że UE nie ma samodzielnych struktur, które mogłyby dostarczyć ekspertów do wsparcia innych krajów w rozwoju narodowych strategii cyberbezpieczeństwa, budowy CERTów czy wzmocnienia systemu prawnego jeśli chodzi o walkę z cyberprzestępczością, musi ona polegać na wsparciu krajów członkowskich, które konkurują o ekspertów nie tylko między sobą, ale także z innymi krajami. Pomysł stworzenia sieci złożonej z placówek badawczych i sektora prywatnego jest właśnie odpowiedzią na tę konkretną potrzebę. Ma to być zaplecze unijne do realizowania nowych projektów w różnych częściach świata.

Czyli nie mówimy tutaj o ekspertach technicznych?

To jest jedno z dużych nieporozumień jeśli chodzi o cyberbezpieczeństwo. Wychodzimy z założenia, że eksperci od cyberbezpieczeństwa to są ludzie, którzy doskonale znają technologię, stale piszą kody i mają tajemną wiedzę o tym jak funkcjonuje internet. W rzeczywistości to grono jest o wiele szersze i obejmuje funkcjonariuszy policji pracujących w oddziałach walki z cyberprzestępczością, prokuratorów, którzy wiedzą jak procedować w przypadku spraw karnych, ale także nauczycieli, pracowników ministerstw, czy obrońców praw człowieka. Zatem tak naprawdę ekspertyza konieczna do budowania bezpiecznej cyberprzestrzeni jest o wiele bardziej różnorodna.

Podsumowując, nie zauważono zwiększonego zainteresowania ze strony polskich instytucji czy organizacji tym obszarem w UE, pomimo, że taka szansa jest?

Jeżeli chodzi o budowanie zdolności cybernetycznych w krajach trzecich to nie. Na usprawiedliwienie instytucji rządowych w Polsce i na świecie należy podkreślić, że dostęp do ekspertów w tym zakresie jest naprawdę bardzo ograniczony. Wszyscy walczą o tych samych ludzi i starają się przede wszystkim zaspokoić własne wewnętrzne potrzeby. Więc to nie jest tylko problem Polski, ale ogólnoeuropejski. Dlatego większość krajów inwestuje poważne pieniądze w stworzenie hubów, gdzie istniejąca wiedza i doświadczenie – niezależnie od tego jak obszerna – jest zbierana i wykorzystywana. Francuzi mają Narodową Agencję Bezpieczeństwa Systemów Informatycznych (ANSSI) oraz Expertise France, która wspiera inicjatywy rządowe poza granicami. Z kolei Estończycy mają RIA, a Koreańczycy KISA.

Czyli nie ma działań na poziomie organizacyjno-instytucjonalno-politycznym. Jest tutaj jeszcze zaplecze do zagospodarowania praktyczne, czyli tworzenie tych ekspertów. Wszyscy zdajemy sobie sprawę, że jest ich brak. Padają od najwyższych szczeblem decydentów w UE stwierdzenia, że w obszarze szeroko rozumianego IT zwłaszcza na odcinku cyberbezpieczeństwa w ciągu 5-8 lat będzie brakować około 300 tys. Co zrobić, jak przekonywać, jak mówić? Dlaczego tyle państw członkowskich tego nie robi i przede wszystkim, co można doradzić Polsce?

Niektóre kraje już to robią. Francja znalazła model, w ramach, którego utworzono kilka centrów badawczych, gdzie budowane jest krajowe zaplecze ludzkie. Mało kto myśli o Irlandii w kategorii znaczącego państwa w cyberprzestrzeni, a jest ona jednym z wiodących centrów jeżeli chodzi o

szkolenie ekspertów od walki z cyberprzestępczością. Uniwersytety w Dublinie stały się tak naprawdę czołówką kuszących placówek edukacyjnych w Europie, które oferują atrakcyjne programy edukacyjne dostosowane do wymogów rynku pracy. Na dodatek, oferowane programy są często zaoczne tzn. osoba nawet nie musi być tam stacjonarnie. Żeby otrzymać dyplom jako ekspert od cyberbezpieczeństwa, może to robić będąc np. w Brukseli.

Czyli można.

Oczywiście, że tak. Trzeba pomyśleć i porównać różne modele oraz zastanowić się, co my możemy zrealizować. Nie byłoby wielkim problemem dla Polski ściągniecie kilku placówek uniwersyteckich w ramach jednej dużej struktury organizacyjnej, która nie musi być scentralizowana ale mogłaby funkcjonować na zasadzie sieci.

Co można byłoby Polsce polecić bazując na tym co się dzieje w Brukseli i na doświadczeniach innych państw UE?

Proponowałbym stworzenie ośrodka, który zgromadzi liczących się ekspertów oraz wiodące placówki badawcze oraz przedstawicieli sektora prywatnego, nie tylko z zakresu bezpieczeństwa, ale także innowacyjności, handlu, edukacji czy polityki rozwojowej. Tylko wtedy możliwe będzie zbudowanie w Polsce całościowego myślenia o cyberbezieczeństwie.

Coś na kształt rozwiązań francuskich?

Na przykład, ale istnieje wiele innych modeli. Czas ucieka, a w ciągu najbliższego roku zostanie wprowadzonych w życie kilka wspomnianych przeze mnie pomysłów, które były ogłoszone przez Komisję w 2017 roku. Byłoby szkoda, gdyby Polska, która ma bardzo dobre szkoły inżynierskie i politechniki, nie wykorzystała tej szansy. Kraje o wiele mniejsze jak Estonia czy Korea Południowa zarabiają olbrzymie pieniądze na budowaniu zdolności w krajach trzecich. To jest inwestycja, która się zwróci.

Dziękujemy za rozmowę

W Brukseli rozmawiali dr Adam Lelonek i dr Andrzej Kozłowski.