aut. Adam Lelonek 07.03.2018

PAWEŁ HERCZYŃSKI: UE BĘDZIE POMAGAĆ W ROZWIJANIU NARODOWYCH ZDOLNOŚCI CYBERNETYCZNYCH [WYWIAD]

O zacieśniającej się współpracy Unii Europejskiej z Sojuszem Północnoatlantyckim i wspólnych ćwiczeniach cybernetycznych, otwartych dialogach cybernetycznych Unii z najważniejszymi państwami świata, cyberdyplomacji, innej wizji Chin i Rosji na rozwój internetu oraz dlaczego Bruksela nie podchodzi entuzjastycznie do propozycji Cyfrowej Konwencji Genewskiej mówił w rozmowie z CyberDefence24.pl Paweł Herczyński, dyrektor Departamentu Polityki Bezpieczeństwa i Zapobiegania Konfliktom Europejskiej Służby Działań Zewnętrznych.

Jaka jest rola Europejskiej Służby Działań Zewnętrznych jeżeli chodzi o działania na arenie międzynarodowej związane z cyberprzestrzenią?

Unia Europejska reprezentuje 28 krajów członkowskich. To jest punkt wyjścia. Wszystko co robimy, zależy od decyzji podejmowanych w gronie tych państw. Oczywiście w ostatnich latach kwestie cybernetyczne nabrały ogromnie na znaczeniu, szczególnie w ostatnim roku, m.in. w związku z różnymi atakami, jak WannaCry czy NotPetya. Również na arenie międzynarodowej kwestie cybernetyczne stały się niezwykle kontrowersyjne, a to ze względu na to, że różne kraje prezentują różny model czy nawet narrację wobec stosunków międzynarodowych w dziedzinie cybernetycznej.

Jakie są to narracje?

Generalnie linia podziału jest niezwykle prosta. Znajduje się ona pomiędzy krajami, które uważają, że internet powinien być otwarty, wolny i dostępny bez żadnych ograniczeń, a pomiędzy krajami, które uważają, że internet powinien podlegać kontroli. Szczególnie aktywne są tutaj Chiny, które forsują idee tzw. *Cyber Sovereignty*, czyli suwerenności cyfrowej.

Podobne podejście ma Rosja.

Federacja Rosyjska wspiera działania Chińskiej Republiki Ludowej. Podobnie robi wiele innych krajów, w których kontrola władz nad internetem jest pochodną metod sprawowania przez nie rządów. Od wielu lat toczyły się na forum ONZ prace w ramach grupy ekspertów rządowych, czyli UN GGE, tj. Group of Governmental Experts. Obrady toczyły się pod parasolem I Komitetu Zgromadzenia Ogólnego. Kilkakrotnie to forum wypracowało pewne niezobowiązujące wytyczne dla zachowań w cyberprzestrzeni. Ostatni UN GGE w 2017 roku nie skończył się jednak przyjęciem rekomendacji. Stało się tak właśnie dlatego, że pojawiły się wspomniane już dwa bloki państw.

Jak to wygląda ilościowo?

Aby dojść do porozumienia w Organizacji Narodów Zjednoczonych potrzebny jest konsensus.

Wystarczy, że jeden kraj się nie zgodzi i już takiego porozumienia nie ma. Generalnie po jednej stronie są m.in. Unia Europejska, Stany Zjednoczone, Kanada, Japonia, Korea Południowa, Australia, czyli grupa, która nazywamy *Like-Minded* – podobnie myślącymi. Po drugiej stronie jest grupa państw Azji Centralnej czy Wenezuela. Jest jednak też kilka krajów, które się wahają, tzw. *Swing States*. Są to na przykład Indie czy Brazylia. Są one z jednej strony rozumieją nasze, tj. zachodnie argumenty, ale są też bardzo wyczulone na stanowisko prezentowane przez Rosję i Chiny. Tak więc mamy ważny i trudny dialog na arenie międzynarodowej na temat w ogóle charakteru internetu. Nie chodzi tylko o wyłącznie o jakąś filozofię jego funkcjonowania, ale i o to, jak prawo międzynarodowe ma się odnosić do cyberprzestrzeni.

Innymi słowy porozumienia nie ma.

Nie ma. Dokładnie to jest grupa krajów, które uważają, że prawo międzynarodowe, zaczynając od Karty Narodów Zjednoczonych, poprzez międzynarodowe prawo humanitarne i ogólnie cały dorobek prawa międzynarodowego, który funkcjonuje *off-line* powinien „z automatu" funkcjonować też *on-line*. Jest też inne podejście, forsowane zresztą nie tylko przez pewne rządy, ale i sektor prywatny. Mówi ono o tym, że należy wypracować nowe zasady prawa międzynarodowego, funkcjonujące w ramach internetu, że potrzeba jest nowej międzynarodowej konwencji.

Firma Microsoft proponuje rozwiązanie, które nazywa Cyfrową Konwencją Genewską. Jak patrzy na to Unia Europejska?

Właśnie do tego zmierzałem. Uważamy, iż firmy prywatne mają pełne prawo do tego, aby brać udział w dyskusji, natomiast kwestia prawa międzynarodowego powinna być domeną dla decyzji państw, a nie prywatnych podmiotów. W przypadku bowiem tych ostatnich oczywiste jest, że kierują się one zyskiem. Jeżeli chodzi o inicjatywę Microsoftu jest ona dość kontrowersyjna. Jest tak dlatego, ponieważ mówienie o tym, iż istnieje potrzeba wypracowania nowych regulacji prawnych dla prawa międzynarodowego, które obowiązywałoby w cyberprzestrzeni, praktycznie automatycznie relatywizuje czy też podważa obowiązywanie obecnego porządku prawnego. Należy także wziąć pod uwagę, że ewentualne prace nad nową konwencją międzynarodową trwałyby lata, jeżeli nie dziesiątki lat i niestety, jak to bywa w przypadku wielostronnych negocjacji, często wymagałoby ogromnych kompromisów. Państwa Unii Europejskiej stoją na innym stanowisku, a mianowicie, że prawo międzynarodowe, które obowiązuje obecnie, powinno mieć zastosowanie tak samo *off-line*, jak i *on-line*. Jesteśmy otwarci na dialog z sektorem prywatnym, natomiast uważamy, że po pierwsze nowe regulacje powinny być domeną państw narodowych, a nie firm prywatnych, a po drugie jest to dosyć niebezpieczna ścieżka, która mogłaby prowadzić do relatywizowania prawa międzynarodowego i jego obowiązywania w cyberprzestrzeni.

Mamy więc klasyczną geopolitykę także i w cyberprzestrzeni. Ale czy biorąc to wszystko pod uwagę, to dialog w ramach ONZu nie będzie kontynuowany?

On jak najbardziej powinien być kontynuowany. W tej chwili jest pewien okres refleksji na temat jak dalej zorganizować i kontynuować międzynarodowy dialog i prace nad normami w cyberprzestrzeni po niekonkluzywnym UN GGE z 2017 roku.

Wcześniejsze kończyły się jakimiś konkretnymi efektami?

Tak, poprzednie obrady grupy eksperckiej były bardzo dobre. Odbyły się one kilkukrotnie w 2013 r. i 2015 r. Wypracowały one cały zestaw norm obowiązujących w cyberprzestrzeni, jak chociażby taką, że żaden kraj nie powinien pozwalać, aby jego terytorium było używane do prowadzenia cyberataków w stosunku do innych państw.

Czy Rosja brała udział w tych obradach?

Jak najbardziej. Podobnie Chiny. Podobnie jak i szereg państw Unii Europejskiej, szczególnie tych, które są najbardziej zaangażowane w dyskusje dotyczące cyberprzestrzeni. Tak jak powiedziałem, w 2017 r. nie udało się zakończyć wielomiesięcznych prac tej grupy w postaci przyjęcia rekomendacji. Jeszcze raz podkreślę, że do tego wymagany jest konsensus i wszystkie państwa muszą się zgodzić. Prace będą jednak kontynuowane.

Ten sprzeciw jest z powodu konkretnych regulacji?

W mojej ocenie chodzi o kwestie fundamentalne odnośnie postrzegania internetu jako takiego. Z punktu widzenia Unii Europejskiej, ale i generalnie – krajów Zachodu kwestie wolności są fundamentalne. Chodzi bowiem o wartości podstawowe, na których zbudowana jest Unia Europejska, czyli prawa człowieka czy prawo do swobodnej wypowiedzi, i nie możemy się zgodzić na to, aby w tej dziedzinie były ograniczenia.

Unia Europejska zaangażowała się w dialog z Chinami w obszarze cyberbezpieczeństwa.

Formalnie mamy sześć dialogów z sześcioma partnerami, które odbywają się regularnie od wielu lat. Jednym z nich jest Chińska Republika Ludowa. Pozostałe to: Stany Zjednoczone, Indie, Brazylia, Japonia i Korea Południowa. Każde z tych państw jest bardzo zaangażowane w kwestie cybernetyczne.

A Izrael?

Oczywiście jest wiele innych krajów, które są niezwykle aktywne. Można wspomnieć chociażby Singapur czy właśnie Izrael. Mamy oczywiście z nimi kontakty. Nie są to jednak formalne dialogi cybernetyczne, które mamy ze wspomnianą wcześniej szóstką.

Czy z Rosją jest podobnie jak z Izraelem czy Singapurem?

Nie. Z Federacją Rosyjską nie jest prowadzony dialog na tematy cyberbezpieczeństwa. Wynika to bezpośrednio ze stosunków na linii Bruksela-Moskwa, które po nielegalnej aneksji Krymu i w związku z destrukcyjną działalnością Rosji na wschodzie Ukrainy zostały ograniczone do bardzo niewielu sfer. Tam, gdzie Unia i Rosja mają pewną zbieżność interesów, ten dialog jest prowadzony, za zgodą państw członkowskich. Natomiast w wielu obszarach od 2014 roku został on znacznie ograniczony. Unia Europejska nie prowadzi z Rosją dialogu w kwestiach cyberbezpieczeństwa.

Jesteśmy po rozmowach z przedstawicielami NATO. Bardzo pozytywnie odnoszą się oni do poszerzającego się zakresu współpracy i partnerstwa pomiędzy Sojuszem a Unią Europejską i jej instytucjami, zarówno na płaszczyźnie technicznej, ale i szerzej. Zresztą Unia podąża tą samą drogą, co NATO – podejście do działań w cyberprzestrzeni, jako kolejnej sfery konfliktu zbrojnego, znalazło swoje odzwierciedlenie w Unii. Jak to wygląda z Pana punktu widzenia?

Zacząłbym od tego, że zarówno NATO i jak Unia Europejska mają swoje siedziby w Brukseli. Przez wiele lat kontakty między oboma organizacjami były jednak niezwykle ograniczone. To się radykalnie zmieniło od Szczytu NATO w Warszawie, kiedy to podpisano wspólną deklarację pomiędzy Sekretarzem Generalnym Sojuszu a Przewodniczącym Rady Europejskiej i Przewodniczącym Komisji Europejskiej, którą nazywamy „Deklaracją Warszawską”. Od tego momentu rozpoczęła się bardzo intensywna współpraca w szeregu różnych dziedzin. Deklaracja wymienia siedem głównych obszarów współpracy, a jako trzeci obszar wymienione są kwestie cybernetyczne. W praktyce wygląda to tak, że mamy regularne kontakty *Staff-to-Staff*, czyli pomiędzy kolegami i koleżankami zajmującymi się

kwestiami cybernetycznymi obu organizacji. Staramy się też wspólnie ćwiczyć. W zeszłym roku, na jesieni 2017 roku po raz pierwszy doszło do wspólnych ćwiczeń Unii Europejskiej i NATO. Wtedy za scenariusz i koordynację działań odpowiadał Sojusz, a my współpracowaliśmy przy całym wydarzeniu. W tym roku natomiast, w listopadzie, to Unia Europejska będzie miała przewodnictwo w tych wspólnych pracach. Aspekty cybernetyczne w tych ćwiczeniach były bardzo ważne . Nie chodzi więc wyłącznie o współpracę *Staff-to-Staff*, nie chodzi tylko o współpracę EUCERT i natowskiego NCERT, czyli komórek, które na bieżąco badają to, co dzieje się w cyberprzestrzeni i natychmiast informują się wzajemnie o pojawiających się zagrożeniach, ale również ćwiczymy i procedury reagowania kryzysowego w przypadku zagrożeń cybernetycznych w postaci dorocznych ćwiczeń, za które w tym roku po raz pierwszy odpowiedzialna będzie Unia Europejska.

Te ćwiczenia mają charakter wyłącznie techniczny? Czy biorą w nim udział również politycy i decydenci?

Jak najbardziej miały charakter i taki i taki. Po stronie UE zaangażowany był Komitet Polityczny i Bezpieczeństwa [Political and Security Committee, PSC – przyp. red.]. Polegało też m.in. na tym, że wspólnie z kolegami z NATO opracowywaliśmy scenariusz, oczywiście całkowicie fikcyjnego, trwały wielomiesięczne przygotowania, a potem przez ponad dwa tygodnie ćwiczyliśmy, łącznie z zaangażowaniem decydentów w krajach członkowskich, zarówno po stronie Unii, jak i NATO.

A jak wygląda kontekst strategicznej współpracy ze Stanami Zjednoczonymi?

Jak już wspomniałem, są one jednym z sześciu partnerów, z którymi posiadamy formalny dialog w kwestiach cybernetycznych. Jest on bardzo pogłębiony. Bardzo mocno trzeba podkreślić, że USA należą do grupy nie tylko bliskich partnerów, ale i tych „podobnie myślących". Są oczywiście pewne różnice. My jesteśmy grupą 28 krajów i w ramach Wspólnej Polityki Zagranicznej i Bezpieczeństwa jakakolwiek reakcja czy aktywność Unii Europejskiej jest możliwa tylko wtedy, kiedy wszystkie państwa członkowskie wyrażą na to zgodę. Często więc Stany Zjednoczone mogą dużo szybciej i dużo sprawniej zabrać głos w danej kwestii, niemniej jednak myślimy podobnie. Powiem nieskromnie, że są dziedziny, w których wyprzedzamy USA.

Jakie na przykład?

Jestem dumny z tego, iż w zeszłym roku Unia Europejska wypracowała i uzgodniła w gronie 28 państw członkowskich to, co nazywamy Cyber Diplomacy Toolbox (CDT). Na chwilę obecną nie został on jeszcze zastosowany, natomiast uzyskaliśmy zgodę wszystkich członków, że jakiekolwiek zagrożenia czy atak cybernetyczny jest traktowany dokładnie w taki sposób, jak jakiekolwiek inne zagrożenie. Znaczy to na przykład, że w przypadku zewnętrznego ataku cybernetycznego, jeżeli byłaby wola krajów członkowskich, możemy zastosować wszystkie działania z zakresu Wspólnej Polityki Zagranicznej i Bezpieczeństwa, w tym sankcje. Te działania mogą polegać na oświadczeniu, które krytykowałoby wrogie działania cybernetyczne, mogą to być wspólnie uzgodnione przez państwa członkowskie konkluzje, mogą to być różne środki nacisku czy presji dyplomatycznej w stosunku do kraju trzeciego , a wreszcie, jeżeli byłby co do tego konsensus – sankcje. Teoretycznie więc mamy możliwość wprowadzenia sankcji w odpowiedzi na atak cybernetyczny.

Czy zdefiniowane zostały kryteria ataku, w oparciu o które można wykorzystać takie środki? Ponieważ jeden atak może polegać na włamaniu się na stronę internetową, a inny na wyłączeniu elektrowni.

To wszystko zależy od państw członkowskich. Jeżeli jedno lub jakaś ich grupa poproszą o użycie istniejących mechanizmów, które Unia ma do dyspozycji, to jest taka możliwość, łącznie z wykorzystaniem sankcji. Kluczowym problemem jest tutaj kwestia atrybucji. Tutaj mamy oczywiście

pewien problem. W przypadku ataków cybernetycznych atrybucja często wymaga czasu i wcale nie musi być w 100% pewna. Nad tym trwają obecnie prace, które będą kontynuowane, w celu wspólnego uzgodnienia pewnych mechanizmów, w tym tego, jaki jest stosunek między atrybucją a użyciem środków z CDT. Kilka tygodni temu mieliśmy atrybucję ransomware'a NotPetya ze strony kilku państw członkowskich. Pierwsza była Wielka Brytania. Jej atrybucja została poparta przez kilka innych państw. W ostatnich dniach mieliśmy też dyskusję w gronie państw członkowskich czy Unia nie powinna użyć jednego z instrumentów CDT. Będzie ona kontynuowana w najbliższych tygodniach.

Regulacje wykorzystania instrumentów Wspólnej Polityki Zagranicznej i Bezpieczeństwa w kontekście zagrozeń cybernetycznych są w jakiś sposób opisane? Jest to jawne?

Jeden z dokumentów, który to określa, to Konkluzje Rady Ministrów (Foreign Affairs Council) z czerwca 2017 roku, jest to ogólnodostępny dokument, jawny. Mamy też dokument niejawny – Implementing Guidelines. On także został uzgodniony pomiędzy wszystkimi państwami członkowskimi. To jednak nie jest koniec, gdyż kluczowym, nadal otwartym tematem, jest kwestia atrybucji.

Podsumowując, to państwo członkowskie zgłasza na forum Unii, że zostało zaatakowane i jak poważna jest skala ataku.

Tak, to dane państwo prosi o pomoc. Po tym wszystkie 28 krajów członkowskich decyduje czy i jak pomóc.

A jak wygląda sytuacja związana z odpowiedzią na cyberatak własnymi działaniami ofensywnymi w cyberprzestrzeni?

Tym się Unia Europejska nie zajmuje. Mogą się tym zająć indywidualnie państwa członkowskie. Unia nie rozwija możliwości ofensywnych.

Czy w Unii Europejskiej panuje przekonanie o tym, że należałoby wzmocnić europejskie *soft power* w obszarze cybernetycznym i konkurować z USA o palmę pierwszeństwa w aktywnościach z nim związanych na poziomie globalnym, w tym z oddziaływaniem na tzw. Swing States?

Prowadzimy wspomniane sześć dialogów, w tym z Brazylią i Indiami. Mają one bogaty dorobek jeżeli chodzi o kwestie związane z cyberbezpieczeństwem. Są one teoretycznie blisko naszego podejścia w kwestiach obowiązywania prawa międzynarodowego, norm czy środków budowania zaufania w cyberprzestrzeni. Pozostają jednak równocześnie pod ogromnym wpływem narracji chińsko-rosyjskiej. Należą one do tzw. grupy BRICS. M.in. i dlatego rozwijamy z tymi krajami dialog, aby przedstawiać i przekonywać do naszej wizji internetu i cyberprzestrzeni.

Na konferencji CYBERSEC, która odbyła się w ubiegłym roku w Krakowie, komisarz ds. unii bezpieczeństwa sir Julian King stwierdził, że do 2022 r. w UE będzie brakować ok. 300 tys. specjalistów w obszarze cyberbezpieczeństwa. Czy są już jakieś konkretne rozwiązania, aby temu przeciwdziałać?

To bardzo ważne pytanie. Te braki nie dotyczą jedynie Unii Europejskiej, ale wszystkich państw, w tym Stanów Zjednoczonych. Zostały podjęte radykalne działania. We wrześniu zeszłego roku została przyjęta i ogłoszona przez Przewodniczącego Komisji Europejskiej Strategia Rozwoju Cybernetycznego Unii Europejskiej, nazywana CyberSecurity Package. Jedną z głównych idei w ramach tego Pakietu jest stworzenie sieci i centrum bezpieczeństwa cybernetycznego, czyli Network of Cybersecurity Competence Centers (NCCC) with a European Cybersecurity Research and Competence Center. Nad tym pracują koledzy z Komisji Europejskiej, z DG Connect [Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii Komisji Europejskiej, ang. Directorate General for

Communications Networks, Content & Technology – przyp. red.]. Dla nas, w Europejskiej Służbie Działań Zewnętrznych, bardzo ważne jest szkolenie i trening z dziedziny bezpieczeństwa cybernetycznego. Do tego kilka tygodni temu wraz z państwami członkowskimi podjęliśmy decyzję, aby agencja, która nazywa się Europejskie Kolegium Bezpieczeństwa i Obrony [European Security and Defence College, ESDC – przyp. red.] rozszerzyła swoją działalność również na kwestie cyberbezpieczeństwa. Na razie pierwszym krokiem będzie szkolenie ekspertów z dziedziny cyberbezpieczeństwa i cyberobrony na potrzeby misji i operacji Unii Europejskiej, natomiast w dalszej perspektywie plany są bardzo ambitne. ESDS ma podjąć się szkoleń znacznie szerzej, dla państw członkowskich, w tym dla ekspertów z dziedziny cyberbezpieczeństwa. Przy czym trzeba pamiętać, że Kolegium jest w swojej istocie siecią instytucji. W jej ramach ma miejsce organizacja, identyfikacja i mapowanie tego, co robione jest przez różne państwa członkowskie. Za jej pośrednictwem podejmowane są starania mające na celu umożliwienie wszystkim krajom członkowskim korzystanie z tego, co oferują niektóre kraje Unii.

Czyli można mówić o pojawianiu się nowych bodźców instytucjonalnych, prawnych i politycznych dla wspierania indywidualnych, krajowych działań z zakresu cyberbezpieczeństwa w ramach Unii Europejskiej.

Zdecydowanie. Cała idea powołania sieci i centrum bezpieczeństwa cybernetycznego służy temu, aby pomóc państwom członkowskim w rozwijaniu narodowych zdolności oraz aby je rozprzestrzeniać na wszystkie państwa Unii Europejskiej. Trzeba tylko pamiętać, że jest to projekt, który dopiero się zaczął.

Rozmawiali dr Andrzej Kozłowski i dr Adam Lelonek