SZEF CYBEROBRONY NATO: „JESTEŚMY TAK SILNI JAK NASZE NAJSŁABSZE OGNIWO” [WYWIAD]

O powołaniu Centrum Operacji NATO w Cyberprzestrzeni, zdolnościach ofensywnych Sojuszu oraz szczycie w Brukseli w 2018 roku w kontekście cyberbezpieczeństwa mówił w rozmowie z CyberDefence24.pl szef sekcji cyberobrony Sojuszu Północnoatlantyckiego Christian-Marc Lifländer.

CyberDefence24: Bardzo żywo dyskutowanym w mediach tematem była nowa struktura dowodzenia NATO czyli Centrum Operacji NATO w Cyberprzestrzeni. Jaka jest jego rola i jak ta jednostka jest umiejscowiona w całej infrastrukturze Sojuszu w kontekście cyberbezpieczeństwa?

Przede wszystkim należy zwrócić uwagę na powód, dla którego taka komórka jak NATO's Cyber Operations Center została utworzona. Należy cofnąć się do Szczytu Sojuszu w Warszawie, podczas którego NATO uznało cyberprzestrzeń za kolejną sferę działań operacyjnych. Chcemy realizować cyberobronę nie tylko z perspektywy technicznej czy obrony sieciowej, lecz i z punktu widzenia zabezpieczenie naszych misji w tym obszarze.

Bardzo często próbuje się to wyjaśniać w taki sposób: od zabezpieczenia informacji, do zabezpieczenia misji. Innymi słowy od ochrony informacji technicznych do bycia w stanie operowania w tej sferze. Oznacza to również, że istotne zmiany muszą zostać wprowadzone w strukturze organizacyjnej. Dlatego też powstało Centrum Operacji w Cyberprzestrzeni. Zachęcam jednak do tego, aby nie skupiać się wyłącznie na tej zmianie, gdyż są i inne.

Jakie na przykład?

Wydaje mi się, że patrzymy na konieczność gruntownej zmiany podejścia do cyberbezpieczeństwa i musimy sobie odpowiedzieć na następujące pytania: czy mamy odpowiednią doktrynę?, czy mamy właściwą strukturę organizacyjną, jak Centrum Operacji w Cyberprzestrzeni?, czy mamy zastosowane odpowiednie elementy edukacyjne i treningowe, których celem jest przygotowanie naszych ludzi, działających w cyberprzestrzeni? I tak dalej. Tak naprawdę więc, jeżeli patrzymy na całe szerokie spektrum zmian, to jest ono bardzo obszerne. Początkowo wskazywaliśmy, że realizacja celów z tym związanych zajmie nam parę lat, lecz z mojej perspektywy jest to transformacja, a nawet powiedziałbym – fundamentalna transformacja, która może zająć nam nawet więcej czasu. Spoglądając na to w jeszcze inny sposób – w tej kwestii nie ma raczej określonego punktu końcowego. Tym, co będzie przez nas kontynuowane, to stała transformacja.

Odnosząc się do tego, w jakim miejscu obecnie się znajdujemy jeżeli chodzi o CYOC to trzeba wrócić do deklaracji ze Szczytu NATO w Warszawie i uznania cyberprzestrzeni za kolejną sferę działań operacyjnych, to w ramach Centrum jesteśmy dopiero w fazie początkowej projektu.

NATO dopiero rozpoczyna szerszy proces?

Jeżeli chodzi o Centrum Operacji w Cyberprzestrzeni – tak. NATO nie stworzy czegoś na kształt cybernetycznego centrum dowodzenia działającego w Stanach Zjednoczonych. Oddzielne dowództwo nie zostanie ustanowione. Ten podmiot ma funkcjonować w ramach istniejących struktur Sojuszu. Jeżeli zaś chodzi o role, zakres odpowiedzialności czy sposób w jaki CYOC będzie wykonywał swoje zadania, to trwają prace w tym zakresie. Innymi słowy, ostatecznym celem jest zapewnienie, że Naczelny Dowódca Sojuszniczy w Europie [*Supreme Allied Commander Europe*, SACEUR – przyp. red.] będzie wyposażony we wszystkie potrzebne narzędzia do podejmowania działań w cyberprzestrzeni. To jest cel CYOC.

Wspomniał Pan Szczyt NATO w Warszawie z 2016 roku. Zbliżamy się do kolejnego, który odbędzie się w tym roku w Brukseli. Jakich decyzji możemy się spodziewać w kwestiach cyberbezpieczeństwa?

Patrząc na obecne wydarzenia, najwyższym priorytetem jest odporność [*Resilience* – przyp. red.]. Wracając jeszcze krótko do Szczytu w Warszawie, to zapadły na nim dwie ważne decyzje. Poza wspomnianym uznaniem cyberprzestrzeni za kolejną sferę działań operacyjnych, była też druga. Chodziło o położeniu większego nacisku na wzmacnianie odporności w sferze cyber na poziomach narodowych [*National Cyber Resilience* – przyp. red.]. Było to Zobowiązanie w zakresie Obrony Cybernetycznej [*Cyber Defence Pledge* – przyp. red.]. W Warszawie udało się nam uruchomić ten projekt.

Podczas tegorocznego Szczytu po raz pierwszy oceniany będzie postęp dokonany w tej sferze, w odniesieniu do przyjętych bazowych kryteriów , przedstawionej w zeszłym roku. Jesteśmy bardzo zainteresowani tym, aby na poziomie państw członkowskich zapewnić realizację postępów. Jesteśmy też gotowi przeznaczać na ten cel potrzebne zasoby, zarówno natury finansowej, jak i niefinansowej, jak na przykład zasoby ludzkie.

Wszyscy stoimy w obliczu tych samych wyzwań: jak przyciągać osoby utalentowane, jak je pozyskiwać i jak je rozwijać jeżeli chodzi o sferę cyber. Wydaje mi się, że jest to jedna z najważniejszych kwestii dla wszystkich państw członkowskich na poziomach krajowych. Kolejne kwestie to chociażby: zapewnienie niezbędnych środków na kwestie cybernetyczne, określenie tego jak ma wyglądać to, co jest „dobre" i ile trzeba za coś zapłacić, żeby uznać to za „dobre" w obszarze cyberobrony czy jak mamy zapewnić świadomość sytuacyjną na poziomie państw członkowskich. To jedne z wielu przykładów. Z podobnymi zagadnieniami pracujemy pomiędzy sojusznikami. To też część składowa Zobowiązania z Warszawy. Ma to zresztą przede wszystkim na celu pomoc państwom członkowskim w identyfikacji najlepszych praktyk narodowych, czyli co działa, a co nie, ale i wspieranie przemian krajowych. Tak więc jednym z rezultatów, bo tak bym to nazwał, a nie decyzją jako taką, jest raport dla szefów państw i rządów wynikający ze Zobowiązania w zakresie Obrony Cybernetycznej. To on właśnie odpowiada na pytanie gdzie jesteśmy.

W raporcie zawarte będą informacje na temat tego jakie postępy poczyniły kraje członkowskie na odcinku cybernetycznym?

Dokładnie. Oceniany będzie okres implementacji decyzji. Identyfikowane będzie to, gdzie mamy progres, a gdzie braki.

Raport będzie jawny?

Nie, będzie on utajniony. W mojej ocenie jego treść będzie czymś, co pozostawać będzie jednak w umysłach szefów państw i rządów. Krajowa odporność cybernetyczna [*Cyber Resilience* – przyp. red.] jest tym, co jest priorytetową potrzebą dobrego poziomu obrony. To też kolejny rezultat Szczytu w Warszawie.

Dane z raportu będą utajnione. Czy jednak są jakieś szacunki lub oceny tego, który kraj jest np. liderem w kwestiach adaptowania zaleceń i transformacji swojej polityki w sferze cyber? Jest jakieś państwo lub grupa państw, które robią zdecydowanie więcej niż inni?

Z mojego prywatnego punktu widzenia, żaden kraj nie jest gotowy na cyberataki [*Cyber Ready* – przyp. red.]. Niektóre oczywiście radzą sobie lepiej niż pozostałe. Nie chodzi tu jednak o indywidualnych zwycięzców. Jeżeli spojrzymy na wszystkie 29 państw członkowskich Sojuszu Północnoatlantyckiego, wyzwania przed którymi stoimy, są podobne dla wszystkich. Podkreśliłbym w sposób szczególny fakt, że nikt nie jest tak naprawdę odporny wobec zagrożeń pochodzących z cyberprzestrzeni. Dlatego właśnie mówię, że dla mnie żadne państwo nie jest w pełni gotowe. Jak powiedziałem wcześniej, to pewien sposób myślenia – nie widzę konkretnego, jasnego punktu końcowego, po przekroczeniu którego można zadeklarować, że już teraz wszystko będzie w porządku. To nie jest tego typu sytuacja. Wspomniałem też konkretne wyzwania, przed którymi stoimy, jak finansowanie czy świadomość sytuacyjna. Państwa odczuwają też i inne, jak chociażby w obszarze współpracy pomiędzy sektorem państwowym i prywatnym. Ostatecznie więc w kwestiach bezpieczeństwa nacisk nie będzie położony na wykazanie zwycięzców czy przegranych, ale przede wszystkim na identyfikowanie braków i niedostatków, a następnie wskazywanie konkretnych rozwiązań.

Wracając do kwestii rekrutacji i pozyskiwania ekspertów i specjalistów od cyberbezpieczeństwa, wiemy, że jest ich za mało na rynku, a sektor prywatny oferuje znacznie bardzo dobre wynagrodzenie. Jak więc NATO może zachęcić takie osoby do pracy w swoich strukturach?

To jest dobre pytanie. Myślę, że nie osiągnęliśmy jeszcze stanu równowagi rynkowej. Jesteśmy wciąż w momencie, kiedy popyt wciąż znacząco przewyższa podaż. Wszyscy poszukują tych samych utalentowanych osób. Mimo to są jednak pewne rzeczy, które mogą zrobić zarówno Sojusz, jak i państwa członkowskie. Jedną z nich jest wyjątkowa misja. Jeżeli chodzi o to, co ludzie pracujący dla takiej organizacji jak NATO mogą robić, to jest to jednak jedyne w swoim rodzaju. Ta misja znacząco różni się od tego, co jest w sektorze prywatnym czy innych miejscach.

Kolejną atrakcyjną cechą, na którą zwraca się coraz większą uwagę i coraz bardziej się docenia, jest szkolenie. Właściwie to szkolenie i edukacja. Posiadanie certyfikatów w danej specjalizacji, co później, miejmy nadzieję, będzie mogło zostać wykorzystane w dalszej karierze, na innych swoich stanowiskach. Innymi słowy: natura misji, szkolenie i edukacja są tym, co możemy dostarczyć ludziom zainteresowanym pracą dla takiej organizacji jak nasza. Zdaje sobie jednak sprawę, że konkurowanie z sektorem prywatnym jest trudne – w sferze honorariów, pensji czy innych kwestii. Myślę, że NATO czy aparaty bezpieczeństwa państwa na poziomach krajowych muszą być nieco sprytniejsze jeżeli chodzi o przykuwanie zainteresowania osób, które mogłyby być zainteresowane pracą dla takich organizacji jak nasza.

Czy NATO prowadzi programy lub działania z niezależnymi hakerami polegające np. na hakowaniu sieci komputerowych w stylu amerykańskiego *Hack the Pentagon*, aby weryfikować poziom ich zabezpieczeń? Są w ogóle takie pomysły?

Ja osobiście nie mam wiedzy o czymś podobnym na poziomie NATO. Jest powód, dla którego może to nie mieć miejsca. Mianowicie jest to bezpośrednio związane z kwestiami prawnymi. Istotnie jest taka inicjatywa jak *Hack the Pentagon*. Myślę, że państwa członkowskie myślą o uruchomieniu podobnych programów u siebie. Z mojego punktu widzenia, patrząc na to zjawisko, może być to interesujące. Może to wprowadzić „do gry" także nowe talenty. W tym wszystkim nie chodzi bowiem tylko o identyfikację ludzi, którzy są już wyprofilowani i zainteresowani kwestiami cyber, ale i otwarcie się na innych, na ten potencjalny rynek, który istnieje, a do którego jeszcze nie udało się dotrzeć. Ale przede

wszystkim to wszystko zaczyna się na poziomie krajowym.

Realizowaliśmy już pewne programy, poprzez które próbowaliśmy wykorzystywać innowacyjne rozwiązania poprzez Agencję NATO ds. Komunikacji i Informacji [*NATO Communications and Information Agency*, NCIA – przyp. red.]. W ramach tych działań dosyć często przyglądamy się także innowacyjnym produktom, głównie pochodzącym z małych i średnich przedsiębiorstw oraz analizujemy w jaki sposób mogłyby one być przydatne dla Sojuszu w kontekście wypełniania wymogów operacyjnych, które przed nami stoją.

Pewne kwestie są jednak bardziej kontrowersyjne. Dlatego też programy podobne do Hack the Pentagon muszą jednak rozpoczynać się na poziomach krajowych, zanim zostałyby uruchomione na poziomie organizacyjnym NATO. O ile zresztą w ogóle by do tego miało dojść.

Powracając jeszcze do rezultatów Szczytu NATO w Warszawie. Inną podjętą tam decyzją było zacieśnianie współpracy pomiędzy Sojuszem a Unią Europejską także w kwestiach cyberbezpieczeństwa. W zeszłym roku Komisja Europejska zaproponowała pakiet cyberbezpieczeństwa UE, tj. Cybersecurity Package. Jak wygląda w praktyce współpraca między obiema organizacjami? Jakie następne kroki powinny zostać podjęte?

Mamy porozumienie techniczne w sprawie cyberobrony zawarte pomiędzy NATO Computer Emergency Response Teams a CERT-EU. Tego typu umowy mają bardzo duże znaczenie, ponieważ umożliwiają wymianę informacji w czasie rzeczywistym. Unia Europejska jest również członkiem Platformy wymiany informacji, dotyczących złośliwego oprogramowania [*Malware Information Sharing Platform*, MISP – przyp. red.]. Czyli wszystkie dane, które przesyłamy do MISP, są również dostępne dla UE. I *vice versa*.

Mamy też współpracę daleko wykraczającą poza platformę, jak regularne spotkania pomiędzy różnymi zespołami, gdzie wymieniamy się dobrymi praktykami, wspólnie rozmawiamy o tym, jak wykorzystywać to, co dostrzegamy, pewne istniejące już rozwiązania i jak dzielić się nimi ze sobą. Rezultaty naszej współpracy mają charakter praktyczny i pragmatyczny. W mojej ocenie współpraca na poziomie technicznym funkcjonuje bardzo dobrze. Jesteśmy zainteresowani kontynuowaniem oraz rozszerzaniem tej współpracy w ramach Porozumienia technicznego w jeszcze większym stopniu.

Są oczywiście i inne tematy, które są w zainteresowaniu nas wszystkich. Jednymi z nich są szkolenia i edukacja. Nie dziwi w związku z tym fakt, że NATO ma obecnie kilka inicjatyw z tym związanych w przygotowaniu. Wśród nich są m.in.: inicjatywa Smart Defence czy Multinational Education and Training Center. Mamy Szkołę NATO w Oberammergau [*NATO School Oberammergau* – przyp. red.], posiadamy NATO Communications School w miejscowości Latina, która ma zostać przeniesiona do Portugalii, do miejscowości Oeiras [ma to nastąpić w 2019 roku – przyp. red.], mamy wreszcie Centrum Doskonałości Współdziałania w obronie przed Cyberzagrożeniami [*NATO Cooperative Cyber Defence Centre of Excellence* – przyp. red.] w Tallinie.

Jeżeli spojrzymy na UE, to zmierza ona w podobnym kierunku. Jest ona także zainteresowana rozszerzaniem swojego portfolio z cyberobrony, szkoleń i edukacji w dziedzinie cyberbezpieczeństwa. To jest też jeden z obszarów, w którym jesteśmy bardzo zainteresowani dalszym zwiększaniem komplementarności, tak, aby nie powielać naszych wysiłków z nimi związanych, ale bardziej w jeszcze większym stopniu się uzupełniać.

W dalszej kolejności mamy kwestię ćwiczeń. Prowadzimy na przykład ćwiczenia Cyber Coalition. W zeszłym roku Unia Europejska została po raz pierwszy zaproszona do wzięcia w nich udziału jako uczestnik. Celem tych ćwiczeń jest sprawdzenie jak jesteśmy w stanie reagować na incydenty w cyberprzestrzeni w sposób skoordynowany. Fakt, że UE bierze w nich udział, jest bardzo ważny,

ponieważ jest ona jedną z organizacji, która będzie częścią każdej reakcji na incydent cybernetyczny na poziomie europejskim. Chcemy więc intensyfikować tego typu współpracę, związaną z ćwiczeniami, a więc: szkolenia, edukacja, ćwiczenia.

To poziom techniczny. A co z poziomem strategicznym?

Jeżeli chodzi o coś, co można byłoby określić terminem ćwiczeń strategicznych, to produktem flagowym i zarazem głównym instrumentem są Ćwiczenia zarządzania kryzysowego [*Crisis Management Exercise*, CMX – przyp. red.]. Nie wyodrębniamy jednak przy nich sfery cyber jako czegoś oddzielnego. Wręcz przeciwnie, kwestie cyber są niejako inkorporowane w całość. Warto jednak wspomnieć, że Unia Europejska odpowiedziała Sojuszowi w ten sam sposób – Sekretarz Generalny NATO został zaproszony na unijne ćwiczenia związane z cyberbezpieczeństwem w zeszłym roku.

Te ćwiczenia UE skupiały się przede wyłącznie na kwestiach cybernetycznym w środowisku hybrydowym. To wszystko ma ogromne znaczenie. To są zresztą dwa doskonałe przykłady dialogu na poziomie strategicznym pomiędzy dwoma organizacjami. Nie tylko więc mamy tu współpracę na poziomie operacyjnym, ale i strategicznym.

NATO podkreśla defensywny charakter swoich operacji w cyberprzestrzeni. Wiemy jednak, że po Szczytach w Walii i Warszawie, cyberatak może pociągnąć za sobą odpowiedź w ramach Artykułu 5 Traktatu Północnoatlantyckiego. Jak wyglądają zdolności ofensywne Sojuszu w cyberprzestrzeni?

Istotnie uznana została możliwość kolektywnej odpowiedzi w cyberprzestrzeni i atak w niej nie będzie różnił się od tego konwencjonalnego na lądzie, morzu czy w powietrzu. Jeżeli więc chodzi o potencjalne przywołanie Artykułu 5 i odpowiedź Sojuszu będą zależały od politycznej decyzji, swojego rodzaju *judgment call*, podjętej przez najważniejszy organ decyzyjny NATO – Radę Północnoatlantycką.

W mojej opinii nie ma potrzeby rozpatrywania tej potencjalnej odpowiedzi jako czegoś symetrycznego. Nie trzeba bowiem odpowiadać na cyberatak innym cyberatakiem. Mamy do dyspozycji cały zbiór narzędzi, jak działania dyplomatyczne czy inne, które mogłyby zostać wykorzystane jako odpowiedź.

Jeżeli natomiast chodzi o zdolności ofensywne, czy jak my wolimy o nich mówić – „efekty", to nie ma tu chyba żadnych niespodzianek. Sojusz nie posiada na własność żadnych czołgów, samolotów czy okrętów, bo one wszystkie należą do państw członkowskich i ich sił zbrojnych, włączonych do struktur wojskowych NATO. Jeżeli spojrzymy na cyberprzestrzeń, Sojusz nie będzie rozwijał swoich zdolności ofensywnych. To wciąż pozostaje prerogatywą i suwerennym prawem samych sojuszników, aby je posiadać i rozwijać w ramach swoich narodowych inwentarzy.

Zupełnie inną kwestią jest dobrowolne dostarczanie tych zasobów dla NATO, np. w czasie kryzysów, eskalacji napięć itp. To już zupełnie inna historia. Tutaj przyglądamy się rozwiązaniom zapewniającym takie możliwości, aby państwa członkowskie mogły przekazać swoje własne, suwerenne „efekty" dla Sojuszu na zasadach dobrowolności. Trwają nad tym prace i myślę, że stworzenie takich mechanizmów czy połączeń pomiędzy siłami a strukturą dowodzenia NATO będzie miało miejsce w ciągu najbliższych miesięcy.

Wracając do możliwości powołania się na artykuł 5. Miało miejsce już bardzo wiele różnego rodzaju cyberataków na całym świecie. Czy widzi Pan możliwość, aby któryś z nich, skierowany przeciwko państwu członkowskiemu Sojuszu, mógł zakończyć się kolektywną odpowiedzią NATO?

Ciężko jest mi odpowiedzieć na to pytanie, ponieważ w ten sposób mogę wpłynąć na dyskusję i decyzję podczas posiedzenia Rady Północnoatlantyckiej. Politycy tam zasiadający bazując na swoich opiniach będą musieli podjąć decyzję, w których przypadkach cyberataku można powołać się na artykuł 5. Musimy pamiętać, że decyzja ta należy do każdego państwa, które po analizie sytuacji może wykorzystać tę opcję. Wtedy reszta członków po własnej ocenie zgadza się lub nie czy dana sytuacja kryzysowa wymaga wykorzystania tego narzędzia. Osobiście wolałbym nie spekulować na ten temat czy któryś z cyberataków, który miał już miejsce na świecie, doprowadziłby do odwołania się do artykułu 5. Po prostu tego nie wiem.

Czy istnieje jakiś plan lub schemat w NATO wskazujący na czynniki, które powinny zostać wzięte pod uwagę?

Moim zdaniem jesteśmy dopiero na początku. Podobna ocena musi mieć miejsce na poziomie Sojuszu, albo również na poziomie państw członkowskich. Przykładowo utrata elektryczności może stanowić przekroczenie progu ataku i zakończyć się powołaniem nie tylko na artykuł 4 ale również na artykuł 5. Każde państwo musi tutaj podjąć samodzielną decyzję. Musimy również pamiętać, że pierwsza odpowiedź ma miejsce na poziomie krajowym. Państwa mają również odpowiedzialność za swoje działania w cyberprzestrzeni. Dlatego tak ważne jest posiadanie obrony na dobrym poziomie, dysponowanie odpowiednimi środkami, żeby uczynić łańcuch bezpieczeństwa NATO możliwie najsilniejszym. Łatwo sobie wyobrazić, że ten sam atak, który może zostać odparty przez państwo o silnej obronie, może sparaliżować słabszego członka Sojuszu. Dlatego chciałbym raz jeszcze podkreślić znaczenie *Resilience*. W NATO jesteśmy tak silni jak nasze najsłabsze ogniwo.

Jak NATO współpracuje z przemysłem w ramach inicjatywy NATO Industry Cyber Partnership, NICP?

Jesteśmy zainteresowani wzajemnymi relacjami z sektorem prywatnym, które przynoszą korzyści obu stronom. Wymieniamy również informacje oraz dzielimy się najlepszymi praktykami. Na poziomie NATO mamy kilka inicjatyw, jak np. Platforma wymiany informacji w przemyśle, dotyczących złośliwego oprogramowania [*Industry Malware Information Sharing Platform* – przyp. red.]. Skupiamy się na aspekcie innowacyjnym. Musimy też podkreślić, że współpracujemy z wieloma aktorami z sektora prywatnego i mamy wielu partnerów z przemysłu. Pracujemy też z małymi i średnimi przedsiębiorstwami. Różni partnerzy dostarczają różne korzyści dla NATO.

Po pierwsze, próbujemy stworzyć platformę, pewien mechanizm, który zachęci partnerów z biznesu do współpracy z nami i dzielenia się informacjami oraz proponowania innowacyjnych rozwiązań z których może skorzystać Sojusz. Jesteśmy również zainteresowani pracami badawczo-rozwojowymi, czyli kiedy poznajemy nowe technologie jak roboty czy sztuczna inteligencja, chcemy zaangażować przemysł, organizacje naukowe i technologiczne w ramach NATO Science & Technology Organization [NATO STO – przyp. red.] oraz innych istniejących forów współpracy.

Wiele osób uważa, że powinniśmy traktować działania w cyberprzestrzeni i działania informacyjne razem. Jedno z bardzo agresywnych wobec Sojuszu państw w swoich działaniach łączy elementy operacji informacyjnych, psychologicznych z obszarem cyber. Jaka jest tutaj perspektywa NATO na ten problem?

Mogę tylko mówić o kwestiach cyberbezpieczeństwa, ponieważ obejmuje to zakres moich obowiązków. W mojej pracy nie ma różnicy kto dokonuje ataków, ponieważ musimy zbudować ochronę i odporność naszych sieci i systemów. Nie ma tutaj różnicy czy mamy do czynienia z aktorami państwowymi czy niepaństwowymi. To, co jest istotne, to fakt, że sieci i systemy NATO są bardzo dobrze chronione i działają bez zarzutu. Wspomniane w pytaniu ujęcie sfery informacyjnej nie należy do mojej pracy i nie mieści się w naszej definicji cyberobrony. Jednocześnie jednak mam świadomość,

że to ma miejsce i nasza praca nad wojną hybrydową jest równie ważna i dotyczy poruszonych tu kwestii. W cyberprzestrzeni głównym celem jest wydobycie informacji, którą można wykorzystać w wojnie informacyjnej.

Zawsze mamy problem z atrybucją ataku. Czy od szczytu w Warszawie w 2016 roku obserwujemy jakieś zmiany w natężeniu ataków o dużej skali przeciwko NATO lub indywidualnym członkom Sojuszu, których autorem są najbardziej agresywne państwa w cyberprzestrzeni takie jak Rosja, Chiny, Korea Północna czy Iran?

Od 2014, czyli od szczytu w Walii, obserwujemy stały wzrost liczby ataków, które są coraz bardziej zaawansowane i zdolne do wyrządzenia poważnych szkód.

Czy może być to związane z pogorszeniem relacji Rosja-NATO i rosyjskiej inwazji na Ukrainę?

To jest bardzo interesujące pytanie i nawiązują do dwóch bardzo ważnych deklaracji, które zostały ogłoszone przez sojuszników przy atrybucji ransomware WannaCry grupie hakerskiej związanej z Koreą Północną i NotPetya Rosji. To są bardzo ważne deklaracje, ponieważ mówią one o zmianie nastawiania wśród niektórych sojuszników. Są oni skłonni publicznie oskarżyć kogoś o autorstwo danego ataku, co w nomenklaturze nosi nazwę „*name and shame*". Uważam, że jest to jedna z rzeczy, która uległa zmianie po szczycie w Warszawie. Państwa są chętne, żeby publicznie powiedzieć: widzimy co robicie i mamy wolę określenia tego publicznie. Nie wiem do jakiego stopnia możemy mówić o zbiorowej atrybucji danego ataku, co byłoby zdecydowanie trudniejsze, ponieważ potrzebujemy mocnych dowodów. Nie tylko muszą one zawierać techniczne dane, ale muszę też zawierać informacje, które pochodzą z wywiadu radioelektronicznego. Jest to też sygnał dla NATO, że sojusznicy poczynili postęp w identyfikacji ataków i ich sprawców.

Czyli widzimy pozytywny trend od szczytu w Warszawie w analizie zagrożeń i przygotowaniach na przyszłość.

Obserwuję obecnie, że sojusznicy przywiązują większą uwagę do cyberbezpieczeństwa. Przeznaczane są też coraz większej zasoby na wzmacnianie cyberobrony, ale musimy pamiętać, że żadne państwo nie jest przygotowane w cyberprzestrzeni. Cyberbezpieczeństwo nie polega na tym, że postawimy krzyżyk przy danej czynności, że ją wykonaliśmy i po prostu o tym zapomnimy. To jest proces, który polega na ciągłym utrzymywaniu gotowości i poprawianiu bezpieczeństwa, również na polu strategicznym.

Bardzo ważna jest komunikacja oraz część informacyjna. Musimy rozwijać normy zachowania państw w cyberprzestrzeni. Musimy sobie odpowiedzieć na pytanie jaki chcemy widzieć w przeszłości internet, jaką cyberprzestrzeń. Czy chcemy żeby była bezpieczna i stabilna? Jakiego rodzaju operacje są dozwolone w tej przestrzeni. Tutaj pojawia się do odegrania rola dla państw i samego NATO. Nie tylko żeby budować odporność, ale też żeby ją stale rozwijać.

Minister obrony Wielkiej Brytanii powiedział, że NATO powinno się przystosować do walki z zagrożeniami hybrydowymi. Co w takim razie powinno być główny priorytetem dla Sojuszu, jeśli chodzi o politykę cyberbezpieczeństwa?

Jeszcze raz to powtórzę, przede wszystkim: odporność, odporność i jeszcze raz odporność. Może to brzmi prosto i głupio, ale łatwiej jest to powiedzieć niż zrobić. Ciągle obserwujemy nowe podatności, jak np. powstałe poprzez IoT. Obszar potencjalnych ataków stale się powiększa. Nie wykluczałbym również tego, że nie jesteśmy świadomi wszystkich obecnych podatności i zagrożeń, o których prawdopodobnie dowiemy się dopiero w przyszłości. Chciałbym jednak uniknąć sytuacji, w której

dyskutujemy nad powołaniem się nad artykuł V w odpowiedzi na to, że czyjaś lodówka została zhakowana. Uważam też, że powinniśmy mieć wszystkie potrzebne narzędzia, ale równie ważna jest bliska współpraca z zagranicznymi podmiotami jak np. Unią Europejską czy państwami partnerskimi.

UE jest bardzo ważna w tym obszarze. Przykładowo niektóre mechanizmy regulacyjne, które zostały stworzone, jak np. sieć wymiany informacji o zagrożeniach czy ostatnio pakiet cyberbezpieczeństwa Komisji Europejskiej, mogą przynieść korzyść także NATO. Moim zdaniem nie mówimy tutaj o grze o sumie zerowej. Szczerze wierzę, że obie organizacją mogą się wzajemnie uzupełniać. Bardzo ważna jest też współpraca z sojusznikami. W cyberprzestrzeni przeszkody geograficzne nie stanowią żadnego problemu. Współpraca z takimi państwami jak Japonia, Korea Południowa czy generalnie z krajami regionu Azji i Pacyfiku są bardzo istotne.

Czy mówimy tutaj głównie o współpracy technicznej?

Tak, dokładnie.

Jak przebiega współpraca z Ukrainą, które jest często przez ekspertów postrzegana jako poligon doświadczalny dla Rosji?

Ukraina jest bardzo ważna. NATO prowadzi Cybersecurity Trust Fund, który jest naszym głównym narzędziem wspomagania Ukrainy w budowaniu skutecznej cyberobrony. Ilość rzeczy, którą musimy jednak zrobić jest po prostu olbrzymia. Szkolimy całe jednostki, prowadzimy działalność edukacyjną czy staramy się poprawić współpracę między poszczególnymi agencjami. Jest to proces ciągły i nie widać jeszcze jego końca. Ponadto dostarczamy Ukrainie konkretnych zdolności i rozwiązań.

W kwaterze głównej NATO w Brukseli rozmawiali dr Andrzej Kozłowski i dr Adam Lelonek.