Rozmowa z dr. Martinem C. Libickim, ekspertem ds. bezpieczeństwa*

Dominika Dziwisz

Obok tradycyjnie rozumianych wymiarów wojny, czyli lądu, morza, powietrza i przestrzeni kosmicznej, coraz częściej wymienia się piąty, jedyny wymiar wojny stworzony w całości przez człowieka – cyberprzestrzeń. Utworzenie Dwudziestej Czwartej Armii Powietrznej USA (24 Air Forces Cyber, AFCYBER), a następnie Cyber Dowództwa USA (United States Cyber Command, USCYBERCOM) pokazuje jak dużą wagę do dominacji w cyberprzestrzeni przykładają dowódcy najpotężniejszej armii świata. Każdego roku rządy państw wysokorozwiniętych wydają dziesiątki miliardów dolarów na zabezpieczenie cywilnych i wojskowych systemów informatycznych. O rzeczywistej skali zagrożenia pochodzącego z cyberprzestrzeni i o tym, czy wojny w XXI w. zostaną przeniesione w ten wymiar Dominika Dziwisz rozmawia z Martinem Libickim, ekspertem z RAND Corporation.

Dominika Dziwisz: Na początku swojej prezydentury Barack Obama powiedział, że „zagrożenie cyberprzestrzeni jest jednym z najpoważniejszych wyzwań dla bezpieczeństwa gospodarczego i krajowego, przed którymi stoi naród amerykański", a „dobrobyt gospodarczy Stanów Zjednoczonych Ameryki w XXI w. będzie zależał od cyberbezpieczeństwa"[1]. Tym samym nadał bezpieczeństwu w cyberprzestrzeni charakter priorytetowy. Jaką ocenę wystawiłby Pan administracji B. Obamy za dokonania w tej dziedzinie?

Martin Libicki: Oceny można dokonać na dwa sposoby. Po pierwsze, oceniając jak Biały Dom radzi sobie z reagowaniem i rozwiązywaniem bieżących problemów. Z drugiej strony należy pomyśleć o tym, co mogło być zrobione dla cyberbezpieczeństwa, a z czym B. Obama sobie nie poradził. Problem z cyberbezpieczeństwem polega na tym, że jest to jeden z tych obszarów, w którym

* Tłumaczenie z języka angielskiego Dominika Dziwisz.

[1] *Remarks by the President on Securing our Nation's Cyber Infrastructure*, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure, 29 maja 2009 r., (dostęp: 10 czerwca 2009 r.).

rozwiązania dopiero zostaną wypracowane. Jakość cyberbezpieczeństwa zależy przecież głównie od decyzji podejmowanych przez gigantów IT, takich jak Microsoft, czyli tak naprawdę kluczowe decyzje podejmowane są przez sektor prywatny, a nie urzędników Białego Domu. Innym powodem impasu decyzyjnego na najwyższych szczeblach władzy jest konflikt trzech grup interesu, czyli wojskowych, którzy problem cyberprzestrzeni rozpatrują jedynie w kategoriach wojny, Departamentu Bezpieczeństwa Krajowego, który koncentruje się na cyberterroryźmie czyli działaniach ludzi, którzy nie lubią Ameryki oraz specjalistów od przestępczości cybernetycznej. Nie ma natomiast żadnej grupy, która rozpatrywałaby cyberbezpieczeństwo jako formę konkretnej, szkodliwej inżynierii. Posłużę się tutaj przykładem. Kiedy człowiek zbudował okręt i nauczył się żeglować, to opanował morze. Potem zaczął prowadzić na morzu wojny. Kiedy człowiek wynalazł samolot i opanował powietrze, to zaczął prowadzić wojny i tutaj. Tak samo było z wykorzystaniem przestrzeni kosmicznej, kiedy wystrzeliliśmy na orbitę satelity militarne. Morze, powietrze i przestrzeń kosmiczna zostały wykorzystane w celach wojskowych, jak tylko wynalazki technologiczne umożliwiły ich eksploatowanie. Natomiast cyberprzestrzeń jest jedyną domeną wojskową, której człowiek nigdy nie opanował. Oprogramowanie zawiera w sobie błędy i to zwykle właśnie one umożliwiają przeprowadzenie ataku.

D. D.: Czy to znaczy, że każdy cyberatak przeprowadzany jest z wykorzystaniem słabości oprogramowania?

M. L.: Nie każdy. I właśnie tutaj pojawia się pytanie, co w takim razie zdziałał prezydent B. Obama. Odpowiedź brzmi: nawet nie zaczął nic robić. B. Obama traktuje problem cyberbezpieczeństwa wyłącznie w kategoriach wojny, terroryzmu i przestępczości internetowej. A tak naprawdę każdy zdaje sobie sprawę, że najbardziej należy się martwić o bezpieczeństwo w sektorze prywatnym. A tak się składa, że przedsiębiorstwa nie potrzebują rad Waszyngtonu jak zarządzać swoimi sieciami. I nie ma żadnego sposobu, aby zmusić ich do zarządzania tymi sieciami tak, jak chce tego D.C.

D. D.: Czyli administracja ma związane ręce…

M. L.: Wszystkie raporty komisji rządowych od 1997 r. mówią to samo, czyli o potrzebie koordynacji, dzielenia się informacją, budowie partnerstwa publiczno-prywatnego i zaufania. I nie można z tym polemizować. Zasada jest taka, że jeśli zarekomenduję, że X albo nie X jest absurdalne, to i tak nie wniosę nic nowego do dyskusji nad cyberbezpieczeństwem. Można wysnuć

smutną konkluzję, że ostatnie 15 lat poświęciliśmy na mówieniu o niczym, bo w gruncie rzeczy ten problem jest dla nas nieuchwytny. Tak więc oceniając B. Obamę należy mu przyznać, że doskonale rozpoznał ten problem, ale nie zrobił zbyt wiele aby go rozwiązać. Jego zasługa polega na wykazaniu, że cyberbezpieczeństwo jest w istocie skomplikowanym problemem. Nie było to łatwym zadaniem.

D. D.: Wynika z tego, że rząd USA dużo mówi o zapobieganiu cyberzagrożeniom, a nie podejmuje żadnych konkretnych działań.

M. L.: Nie ma pośpiechu, bo nie ma bezpośredniego zagrożenia. Co się teraz dzieje i wymaga bieżących działań to kradzież własności intelektualnej. Kradną Chińczycy, ale nie tylko oni. To są oczywiście nielegalne, niesprawiedliwe i złe działania. Jednak z drugiej strony to nie jest największy transfer dóbr jaki świat widział. Bogatsze kraje robią wszystko żeby zarobić jak najwięcej przy najmniejszym nakładzie kapitału i siły roboczej. To jest oczywiste. Jednak, mimo że ktoś kradnie moją wiedzę, to nie zmienia faktu, że tak czy inaczej będę zarabiał. Innymi słowy, jeśli wiem jak zrobić mydło, a ty kradniesz mi tę wiedzę, nie powstrzymuje mnie to od dalszej produkcji mydła. Nawet jeśli złodziej mojej receptury robi to mydło jeszcze wydajniej niż ja. To nie jest dla mnie żaden wyznacznik jakości relacji międzynarodowych.

D. D.: A co nim jest?

M. L.: Na liście warunków relacji chińsko-amerykańskich jest bardzo wiele czynników. Chcemy eksportować i importować z Chin, chcemy żeby Chiny powściągały niecne zamiary Korei Północnej i żeby mniej interesowały się niektórymi wyspami na Morzach Południowo- i Wschodniochińskim, chcemy żeby Chiny ograniczyły emisję dwutlenku węgla. Gdzie na tej liście jest cyberprzestępczość? Nie będzie na niej wysoko. A to ogranicza działania Białego Domu. Co więcej, mam przypuszczenie, że tak naprawdę Chińczycy niewiele mogą ukraść z cyberprzestrzeni, bo transfer technologii jest bardzo skomplikowany. Sposobem na powstrzymanie fali kradzieży własności intelektualnej może być przekupienie przeciwnika. Nie mam na myśli zwykłej łapówki, ale propozycję czegoś bardziej atrakcyjnego.

D. D.: Na przykład czego?

M. L.: Na przykład członkostwa w jakiejś wspólnocie narodów. To może zadziałać.

D. D.: Parę tygodni temu Departament Obrony alarmował o rosnącym zagrożeniu cybernetycznym z Iranu…

M. L.: Leon Panetta powiedział, że atakują nas Irańczycy. Zapomniał, że to my zaatakowaliśmy ich pierwsi. A co takiego zrobili? Na kilka dni utrudnili dostęp do bankowości internetowej oraz sprawdzili kilka twardych dysków w Arabii Saudyjskiej. Przepraszam, ale nie ekscytuję się żadnym z tych dokonań. Nie mogę, bo czy to rzeczywiście wszystko co potrafią zrobić terroryści? Wiem doskonale jakie działania terrorystyczne może podjąć Iran. Ataki na banki i wykradzenie informacji z kilku komputerów to jest nic.

D. D.: Czy międzynarodowa konwencja dotycząca bezpieczeństwa cybernetycznego może być skutecznym narzędziem zapobiegania cyberprzestępczości?

M. L.: Nie, nie może. Taka konwencja już istnieje. Nazywa się Konwencją Budapesztańską (*Budapest Convention on Cybercrime*). Jest ona otwarta do podpisu dla państw członkowskich Rady Europy oraz państw, które nie są członkami Rady Europy, ale uczestniczyły w jej opracowywaniu. Wszystko wygląda pięknie jedynie na papierze. Spora część państw, na przykład z byłego ZSRR, jest wylęgarnią sprytnych cyberprzestępców. I tutaj niewiele można zrobić, bo tolerowanie cyberprzestępczości jest dla tych krajów czysto ekonomiczną kalkulacją. Weźmy za przykład Rumunię, w której jest wielu cyberprzestępców, bo jest to dobre dla rumuńskiej gospodarki. Poza Konwencją mamy Rosjan i Chińczyków, których udział w przestępczości internetowej jest największy. Wszystko i tak kończy się na *realpolitik*. Ile można osiągnąć jeśli przyciśnie się te kraje? Odpowiedź brzmi: niewiele. Chyba, że poważnie się zablefuje, na przykład grożąc bronią nuklearną. Problem z *bluffem* polega jednak na tym, że jeśli druga strona nie zastosuje się do naszych żądań, musimy ten *bluff* zrealizować. Jeśli tego nie zrobimy, to przestaniemy być wiarygodni. Kto jednak chce igrać z USA…?

D. D.: Wróćmy do B. Obamy. Na początku swojej prezydentury powołał on cyberkoordynatora, który miał być jego kluczowym doradcą ds. cyberbezpieczeństwa. Jakie są właściwe funkcje koordynatora i czy ma on realny wpływ na kształtowanie polityki cyberbezpieczeństwa?

M. L.: Osobą numer jeden, która ma bezapelacyjnie największy wpływ na politykę cyberbezpieczeństwa w USA jest gen. Keith Alexander, szef Agencji Bezpieczeństwa Narodowego (*National Security Agency*, NSA).

Cyberkoordynator Schmidt spędził sporo czasu w drodze propagując cyberbezpieczeństwo. I to jest jego duża zasługa. A jego następca… cóż… szczerze mówiąc nawet nie wiem jak się nazywa.

D. D.: Niestety ja też nie pamiętam.

M. L.: To tylko potwierdza, co chciałem powiedzieć. Szef Cyber Crime Division w FBI ma więcej władzy, również National Protection and Programs Directorate działający w ramach Departamentu Bezpieczeństwa Krajowego ma więcej władzy, a nawet niektóre szychy w ramach Departamentu Obrony. Ważnymi osobami są Chris Painter i Michel Markoff z Departamentu Stanu.

D. D.: Czy powołanie cyberkoordynatora w ogóle było potrzebne?

M. L.: Myślę, że B. Obama zdał sobie sprawę z tego, że ma bardzo dużo do wykonania. W tym zakresie złożył obietnice i chciał się z nich wywiązać, ale jednocześnie nie przeznaczył na cyberbezpieczeństwo wystarczającego budżetu. Szanse na zwiększenie wydatków na cyberbezpieczeństwo pojawią się dopiero wtedy, kiedy dojdzie do poważnego ataku na USA. Możliwe, że nawet nigdy do tego nie dojdzie. Możemy mieć na tyle szczęścia, że komputery rozwiną się w pożądanym przez nas kierunku. Równie dobrze może być inaczej. I wtedy wszyscy będziemy mieli poważny problem.

D. D.: Nie można mówić o cyberbezpieczeństwie i B. Obamie nie wspominając o Stuxnecie. Nie rozumiem dlaczego przyznano się do ataku…

M. L.: Muszę zaprotestować. B. Obama nigdy nie przyznał się do ataku Stuxnetem. Nigdy nie było oficjalnej deklaracji Stanów Zjednoczonych na temat ataku Stuxnetem.

D. D.: Dlaczego zatem media informują, że to USA dokonały ataku na irańskie instalacje nuklearne?

M. L.: Z dwóch powodów. Po pierwsze, kiedy spojrzeć na naturę tego robaka i to jak wiele pracy włożono w skonstruowanie go, wtedy widać jak na dłoni, że mogły tego dokonać tylko dwa kraje – USA i Izrael. Po drugie, David Sanger z „New York Times" powiedział, że B. Obama był osobiście zainteresowany projektem. W mojej opinii to był bardziej projekt izraelsko-amerykański niż amerykańsko-izraelski. Jest to dla mnie prawie pewne ze

względu na budowę kodu. Po pierwsze, w przeciwieństwie to Amerykanów, Izraelczycy lubią robić wrażenie na swoich sąsiadach popisując się jak bardzo są sprytni. Po drugie, Izrael ma swoje *style points* – użyli nie jednego, ale dwóch skradzionych certyfikatów, czterech luk „zero days" (nieupublicznionych przed atakiem – przyp. aut.), a w kod jeszcze wpisali podpowiedzi. Amerykanie nie robią tego, bo nie zależy im na zrobieniu na kimś wrażenia. Mówię to zupełnie na poważnie. I dlatego właśnie myślę, że Stuxnet był w większości projektem izraelskim.

D. D.: Gdyby to Pan decydował o przeprowadzeniu ataku Stuxnetem…

M. L.: Jeśli ta decyzja należałaby do mnie, zdecydowałbym się go użyć. Z tego powodu, że Iran ma broń nuklearną, której skutki użycia byłyby tragiczne. Nic o porównywalnie tragicznych skutkach nie może się wydarzyć w cyberprzestrzeni. Innymi słowy, broń nuklearna traktowana jest poważnie, broń cybernetyczna jest bardziej bezpieczna.

D. D.: A co z pięknymi deklaracjami B. Obamy na temat wolności w internecie, wolnościami obywatelskimi, zwalczaniu wszelkich form wrogich działań w cyberprzestrzeni?

M. L.: Nie ma żadnej niezgodności między wolnością w internecie i wszystkimi innymi pięknymi wartościami oraz otwartością a wbijaniem szpili Iranowi. Kiedy mówimy o wolności internetu, hipokryzja objawia się przepuszczaniem takich dokumentów jak SOPA (*Stop Online Piracy Act*), który w rzeczywistości uznaje za nielegalną sieć anonimową (TOR, ang. *The Onion Router*), technologię używaną np. przez chińskich obywateli do omijania rządowych zapór internetowych (ang. *firewalli).*

D. D.: Pomijając kto był sprawcą ataku – czy Stuxnet był dobrą taktyką na powstrzymanie produkcji broni nuklearnej?

M. L.: Tak, to była dobra, ale nie doskonała taktyka. Byłaby jeszcze lepsza gdyby Stuxnet lepiej zadziałał. Tym bardziej, że koszt przeprowadzenia operacji był znikomy jeśli porównamy go do operacji militarnych.

D. D.: Dotychczas wymienia Pan same pozytywne aspekty Stuxnetu. Czy jego użycie miało jakieś wady?

M. L.: Po operacji pojawiły się obawy, że kod źródłowy zostanie wykorzystany do ataku na inne cele. Oczywiście do tego nie doszło.

D. D.: Dlaczego?

M. L.: Bo słabości systemu, które wykorzystywał do ataku Stuxnet zostały szybko naprawione. Jeśli by myśleć o Stuxnecie numer dwa, to trzeba znaleźć inne słabości w zabezpieczeniach. Ale nie ma to większego sensu, bo co więcej może zaatakować Stuxnet Dwa? Natura cyberwojny jest taka, że kiedy już zbadamy jak doszło do ataku, to zabezpieczamy to miejsce jeszcze lepiej. Znając triki ofensywy, stosuje się nowe triki w defensywie.

D. D.: Skoro już Pan poruszył temat ofensywy i defensywy. Cyberzagrożenia są traktowane przez rządy państw bardzo poważnie. Nie ma natomiast zgody co do możliwości prowadzenia wojny cybernetycznej. Opinie ekspertów są podzielone.

M. L.: Tak, tak. Załóżmy, że są opinie moja i innych. (*śmiech*)

D. D.: Nie pozostaje mi nic innego niż się z tym zgodzić. Ale jeśli mówimy o „reszcie"… Howard Schmidt twierdzi na przykład, że nie ma czegoś takiego jak cyberwojna, bo w środowisku internetowym nie ma zdecydowanych zwycięzców i przegranych. Dla kontrastu, Richard Clarke wierzy, że skuteczny atak cybernetyczny może pokonać USA w 15 minut. Czy to w ogóle jest możliwe?

M. L.: Większość efektów cyberwojny jest tymczasowych. W lipcu ubiegłego roku huragan odciął prąd w Waszyngtonie na około tydzień. To były najgorętsze dni w roku. Na szczęście byłem wtedy w Kalifornii. Ale na takie zdarzenia trzeba być przygotowanym jeśli się mieszka w Waszyngtonie. Nie da się przewidzieć działań matki natury. Tak samo jest z cyberwojną.

D. D.: Czy ryzyko cyberwojny jest przesadzone?

M. L.: To co mówi Richard Clark, że USA rozpadnie się jak meksykańska piniata jest niedorzeczne. Cyberwojna nie jest w stanie spowodować takich szkód, jak to sobie wyobrażają ludzie. A poza tym jeśli będziemy musieli przejść do ofensywy cybernetycznej, USA są bardzo dobrze przygotowane.

D. D.: Czy tak samo dobrze wygląda defensywa amerykańska?

M. L.: Nie jest źle. Chińczycy są od nas dużo słabsi. Prawdopodobnie jesteśmy w stanie rozłożyć chiński internet bardzo szybko.

D. D.: No tak, ale struktura chińskiego internetu jest inna niż tego w USA. Jest on zarządzany centralnie i między innymi z tego powodu łatwiej go zaatakować.

M. L.: Pozwolę sobie przytoczyć dane statystyczne. Cyberwojna jest prowadzona przez wykorzystanie luk w zabezpieczeniach oprogramowania. Około 98 proc. oprogramowania używanego na świecie stworzyli Amerykanie, co oznacza, że Amerykanie stworzyli 98 proc. luk w zabezpieczeniach jakie mogą zostać wykorzystane do ataku. To daje nam niesamowitą przewagę.

D. D.: Które kraje są zatem największymi graczami w cyberrozgrywce: liderzy w dziedzinie nowoczesnych technologii czy kraje o słabym stopniu skomputeryzowania?

M. L.: Wszystko zależy od celu jaki chce się osiągnąć. Na przykład Rosjanie są bardzo dobrzy. Możliwe nawet, że są tak dobrzy jak Amerykanie. Bo Rosjanie mają sporą rezerwę matematyków zatrudnionych na stanowiskach, na których nie mogą wykorzystywać w pełni swoich umiejętności. Inny powód: mają odpowiedni kapitał ludzki i wiarę w służby specjalne. Również Chińczycy są dobrzy. Nie tak dobrzy jak Rosjanie, bo ich techniki nowoczesnego wywiadu są kiepskie, ale są za to bardzo uparci i nieustępliwi. Także Indie mogą być bardzo dobre, ale tak naprawdę nie mają powodu, żeby być dobrym w tej dziedzinie. Nie wierzą w kradzież własności intelektualnej, tak naprawdę nie obawiają się Pakistanu i nie mają powodu by atakować Chiny. Ale jeśli zajdzie taka potrzeba, Hindusi będą w stanie się zorganizować. Tak samo jak w Rosji, również w Indiach jest duża grupa matematyków zatrudnionych na stanowiskach, na których się marnują. Czyli problem odpowiednich ludzi do tej roboty odpada. Inny cybergracz to Izrael, z którego pochodzą wybitni informatycy. Równie dobra może być Szwajcaria, ale nie ma żadnej potrzeby. Tak samo jest w przypadku Szwecji. Oprócz tej chudej dziewczyny w trylogii Millenium Stiega Larssona (*śmiech*). Singapur również mógłby być poważnym graczem, gdyby miał taką potrzebę.

D. D.: A Japonia? Kraj nowoczesnych technologii…

M. L.: Raczej nie. Wyklucza to filozofia *bushido*, czyli kodeks samurajski. Poza tym dobry haker musi być indywidualistą, a kultura japońska tego nie lubi. Inaczej jest w Izraelu, gdzie każdy jest indywidualistą. Również Polska może być dobra w „cybersprawach". Ale nie ma takiego pragnienia.

D. D.: Cyberdefensywa amerykańska ogranicza się do obrony sektora publicznego. Czy rząd powinien w równym stopniu zabezpieczać sektor prywatny co publiczny?

M. L.: Jeśli mówimy o sektorze energetycznym, to zdecydowanie tak. Jeśli mówimy o korporacji robiącej np. mydło – odpowiedź brzmi nie. To jest ich problem. Dlatego tak ważne jest rozróżnienie infrastruktur na te, które są krytyczne dla państwa i inne.

D. D.: Jak zatem można chronić strategiczne firmy sektora prywatnego?

M. L.: Jeśli chodzi o sektor energetyczny – wprowadziłbym bezwzględny wymóg całkowitego odcięcia systemów kontroli w elektrowniach od internetu. To oczywiście nie będzie bez wpływu na koszty energii elektrycznej, czyli uderzy po kieszeniach obywateli. Ale jest to jedyny sposób, aby wyeliminować ryzyko ataku cybernetycznego. Są jednak elementy infrastruktury krytycznej, które nie mogą działać bez podłączenia do sieci, na przykład telekomunikacja, bo to nie tylko telefony ale i oczywiście internet, albo bankowość, bo w końcu jesteśmy uzależnieni od bankowości online.

D. D.: Kiedy umówiliśmy się na rozmowę myślałam, że będzie mnie Pan przekonywał o nieuchronności cyberwojny…

M. L.: Na pewno nie. Kilkanaście lat temu myślałem inaczej, ale moje poglądy niespodziewanie ewoluowały w odwrotnym kierunku i dzisiaj jestem sceptyczny co do możliwości prowadzenia samodzielnej wojny w tej nowej domenie działań militarnych. John Arquilla jest odmiennego zdania, więc dla równowagi warto z nim porozmawiać.