Michał Grzelak

Międzynarodowa strategia USA dla cyberprzestrzeni

Dotychczasowy rozwój cyberprzestrzeni i zapewnienie bezpieczeństwa tego środowiska nie były konsekwencją przemyślanych strategii opracowanych przez rządy państw czy organizacje międzynarodowe, ale efektem działań społeczności międzynarodowej, przebiegających głównie w sposób niezorganizowany. Rosnąca zależność współczesnego społeczeństwa od technologii sieciowych i stopniowe przenikanie usług oferowanych w cyberprzestrzeni do kolejnych sfer życia ludzi na całym świecie pokazało jednak, że wykorzystanie Internetu jest nie tylko dobrodziejstwem, ale wiąże się też z dużymi problemami. Gwałtowny wzrost liczby zagrożeń w cyberprzestrzeni zapoczątkował dyskusję na temat jej przyszłości. Skłonił też wiele państw i organizacji międzynarodowych do intensywnych działań mających na celu zapewnienie otwartości i bezpieczeństwa Internetu.

Problematyka bezpieczeństwa cyberprzestrzeni jest od pewnego czasu obecna w dyskusji publicznej, a zagadnienia związane z przestępczością, terroryzmem i potencjalną wojną w sieci są przedmiotem opracowań przygotowywanych przez ekspertów ośrodków analitycznych i instytucji publicznych na całym świecie. Poszczególne państwa i organizacje międzynarodowe przygotowują strategie działania, a także tworzą formacje odpowiedzialne za prewencję i reagowanie na incydenty komputerowe. Dotychczasowe działania ograniczały się głównie do projektów krajowych lub tworzonych na poziomie organizacji międzynarodowych. Pomimo wskazywanej przez ekspertów konieczności działania uwzględniającego ponadnarodowy charakter Internetu, nie podejmowano inicjatyw strategicznych czy legislacyjnych na poziomie globalnym. Zapowiedzią zmian w tym zakresie jest nowa strategia USA, która poza sprawami związanymi z bezpieczeństwem cyberprzestrzeni, porusza również kwestie związane z jej rozwojem oraz wykorzystaniem możliwości oferowanych przez Internet na rzecz wspierania wolności, demokratyzacji i budowania pokoju na świecie.

NOWA MIĘDZYNARODOWA STRATEGIA USA DLA CYBERPRZESTRZENI

16 maja 2011 r. administracja Stanów Zjednoczonych zaprezentowała międzynarodową strategię dla cyberprzestrzeni – *U.S. International Strategy for Cyberspace*[1].

[1] *U.S. International Strategy for Cyberspace*, White House, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (dostęp: 23 maja 2011 r.).

O wadze nowego dokumentu świadczy lista osób obecnych podczas jego oficjalnej prezentacji[2] – doradca prezydenta Baracka Obamy do spraw walki z terroryzmem John Brennan, sekretarz stanu Hillary Clinton, sekretarz handlu Gary Locke, prokurator generalny Eric Holder, zastępca sekretarza obrony William J. Lynn III, sekretarz bezpieczeństwa krajowego Janet Napolitano i koordynator do spraw cyberbezpieczeństwa w Białym Domu Howard Schmidt. Zgodnie ze słowami sekretarz H. Clinton, nowa, opracowana we współpracy z 18 amerykańskimi departamentami i agencjami strategia nie jest dokumentem technicznym i nie prezentuje gotowego rozwiązania, ale opisuje raczej wizję przyszłości cyberprzestrzeni, zaproponowaną przez prezydenta Baracka Obamę. Zawiera także propozycje działań, które mają pomóc w urzeczywistnieniu tej wizji. Strategia ma być „mapą drogową" dla amerykańskich instytucji rządowych, których wspólnym celem jest budowa i utrzymanie „otwartej, interoperacyjnej, bezpiecznej i niezawodnej globalnej sieci"[3], której potencjał będzie wykorzystywany przez wszystkich gotowych do współpracy partnerów w celu poprawy dobrobytu społeczeństwa na całym świecie.

Jest to pierwsza globalna strategia, zawierająca propozycję ukierunkowanego rozwoju Internetu. Rozumiejąc, że żadne państwo czy organizacja nie jest w stanie samodzielnie decydować o przyszłości i zapewnić bezpieczeństwa cyberprzestrzeni, Stany Zjednoczone zdecydowały się na budowę sieci międzynarodowych partnerstw z krajami, organizacjami, ośrodkami akademickimi i przedstawicielami sektora prywatnego, pozostając przy tym liderem w dziedzinie rozwoju i utrzymania bezpieczeństwa sieci, a także przewodząc globalnej „cyberkoalicji". W ramach tej struktury USA chcą podejmować przez *consensus* decyzje dotyczące rozwoju Internetu i jego bezpieczeństwa. Chcą także zbudować strefy odpowiedzialności za poszczególne elementy i sfery globalnej sieci w celu uniknięcia dublowania działań poszczególnych podmiotów, co pozwoli uniknąć nieporozumień mogących prowadzić do konfliktów.

Stany Zjednoczone chcą realizować przedstawioną w strategii wizję przyszłości cyberprzestrzeni w siedmiu priorytetowych obszarach działania:

- gospodarce – poprzez wspieranie międzynarodowych standardów, wolnego rynku i ochronę własności intelektualnej;
- ochronie sieci – poprzez zwiększanie bezpieczeństwa, niezawodności i odporności sieci, usprawnienie systemu reagowania na sytuacje kryzysowe, tworzenie międzynarodowych partnerstw i jednolitych norm zachowań w sprawie bezpieczeństwa cyberprzestrzeni;
- egzekwowaniu prawa – poprzez tworzenie międzynarodowej polityki walki z cyberprzestępczością, harmonizowanie prawa dotyczącego cyberprzestępczości, aby było zgod-

[2] H.A. Schmidt, *Launching the U.S. International Strategy for Cyberspace*, The White House Blog, http://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace (dostęp: 25 maja 2011 r.).

[3] *U.S. International Strategy for Cyberspace*, *op. cit.*, s. 5.

ne z konwencją z Budapesztu[4], ograniczenie terrorystom i przestępcom możliwości wykorzystywania Internetu do planowania operacji, finansowania i podejmowania ataków;
- współpracy wojskowej – poprzez dostosowanie sił zbrojnych do nowych zagrożeń w celu zapewnienia bezpieczeństwa sieci wojskowych, tworzenie nowych i wzmacnianie istniejących sojuszy oraz poszerzanie współpracy w zakresie kolektywnej obrony cyberprzestrzeni;
- zarządzaniu globalną siecią – poprzez wspieranie otwartości i innowacji w Internecie, tworzenie bezpiecznej i stabilnej infrastruktury, prowadzenie wielostronnej dyskusji na temat rozwoju Internetu;
- rozwoju międzynarodowym – poprzez tworzenie globalnej społeczności odpowiedzialnej za rozwój cyberprzestrzeni, rozpowszechnianie doświadczeń, wiedzy i umiejętności partnerom USA, rozwój dobrych praktyk, szkolenia dla organów ścigania, prawników i prawodawców, rozwój relacji na szczeblu politycznym i eksperckim;
- wolności Internetu – poprzez wspieranie społeczeństwa obywatelskiego i praw podstawowych, wolności wypowiedzi oraz prawa do stowarzyszania, współpraca z organizacjami pozarządowymi, współpraca na rzecz efektywnej ochrony danych i prywatności oraz zapewnienie wolnego przepływu informacji (m.in. zapobieganie cenzurze w Internecie).

Wymienione obszary działania będą podzielone między departamenty i agencje USA. Wszystkie działania wymagają współpracy rządu Stanów Zjednoczonych z partnerami zagranicznymi i sektorem prywatnym. Ich realizacja będzie przedsięwzięciem łączącym elementy dyplomacji, obronności i działań na rzecz rozwoju sieci.

Rolą dyplomacji, gdzie kluczową funkcję będzie wiódł prawdopodobnie Departament Stanu USA (w departamencie powołano pełnomocnika do spraw cyberprzestrzeni), będzie wykorzystywanie członkostwa w organizacjach międzynarodowych, a także tworzenie nowych dwustronnych i wielostronnych międzynarodowych partnerstw, prowadzenie ponadnarodowej dyskusji oraz rozwijanie i wdrażanie norm dotyczących działania w cyberprzestrzeni.

Rolą obronności, za którą przypuszczalnie będą odpowiedzialne Departament Obrony USA, Departament Bezpieczeństwa Krajowego oraz inne instytucje zajmujące się bezpieczeństwem sieci, będzie tworzenie systemów i procedur pozwalających na zabezpieczenie cyberprzestrzeni przed przestępcami, terrorystami i państwami dążącymi do zakłócenia działania sie-

[4] Konwencja o cyberprzestępczości (*Convention on Cybercrime*), konwencja z Budapesztu, podpisana przez Rzeczpospolitą Polską w listopadzie 2001 r. Jest pierwszym porozumieniem międzynarodowym w sprawie przestępczości komputerowej. Jej celem jest harmonizacja przepisów krajowych dotyczących cyberprzestępczości oraz poprawa technik dochodzeniowych i współpracy międzynarodowej, http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm (dostęp: 25 maja 2011 r.); nieoficjalne tłumaczenie konwencji przygotowane przez Ministerstwo Sprawiedliwości RP, http://conventions.coe.int/Treaty/EN/Treaties/PDF/Polish/185-Polish.pdf (dostęp: 25 maja 2011 r.).

ci. Stworzone zostaną narzędzia pozwalające na skuteczne odstraszanie potencjalnych agresorów, wczesne wykrywanie incydentów komputerowych, a także plany działania umożliwiające ograniczenie i niwelowanie negatywnych skutków ataków.

Ukierunkowany rozwój globalnej sieci ma być zagwarantowany przez działania instytucji, które będą dążyły do budowy cyberprzestrzeni spełniającej kryteria otwartości, interoperacyjności, bezpieczeństwa i niezawodności, a także do poszerzania zasięgu sieci i ułatwiania dostępu do niej w celu poprawy dobrobytu użytkowników Internetu.

Wpisując do nowej strategii elementy związane z ochroną praw do wolności wypowiedzi i stowarzyszania się, Stany Zjednoczone doceniają w ten sposób rolę cyberprzestrzeni w osiąganiu światowego pokoju i szerzeniu zasad demokracji, która była szczególnie widoczna podczas ostatnich wydarzeń w krajach Afryki Północnej i Bliskiego Wschodu. Rezultaty osiągnięte przez tamtejsze grupy opozycyjne nie byłyby możliwe bez udziału mediów społecznościowych i nieskrępowanej wymiany informacji, oferowanej właśnie przez globalną sieć.

USA podkreślają przy tym, że państwa ograniczające wolny przepływ informacji poprzez stosowanie filtrów i zapór sieciowych na poziomie krajowym, stwarzają tylko iluzję bezpieczeństwa, ograniczając przy tym efektywność i rozwój Internetu.

Pewne wątpliwości mogą budzić zapisy dotyczące ochrony prywatności i danych osobowych w świetle pojawiających się oskarżeń o wykorzystywanie sieci do inwigilowania obywateli przez służby specjalne USA, gromadzenie danych osobowych i handel nimi przez amerykańskie firmy (Google, Facebook itp.), a także „cenzurowanie" dostępu do informacji publicznej, pojawiające się m.in. przy okazji publikacji depesz dyplomacji Stanów Zjednoczonych przez portal WikiLeaks.

DZIAŁANIA NA RZECZ CYBERBEZPIECZEŃSTWA

Opisywane w strategii propozycje odnoszą się do szeroko pojmowanej przyszłości globalnej sieci, a kwestia jej bezpieczeństwa jest tylko jednym z elementów, które zdaniem autorów zapewnią zrównoważony rozwój Internetu.

Do spraw związanych bezpośrednio z cyberbezpieczeństwem odnoszą się trzy z opisanych obszarów działania – ochrona sieci, legislacja i egzekwowanie prawa oraz współpraca militarna.

W celu zwiększenia bezpieczeństwa globalnej sieci USA chcą rozwijać współpracę z państwami i organizacjami, a także tworzyć publiczno-prywatne partnerstwa, których celem będzie budowa i ochrona infrastruktury krytycznej oraz tworzenie norm bezpiecznego zachowania w cyberprzestrzeni. Stany Zjednoczone chcą także rozwijać zdolności w zakresie monitorowania, ostrzegania oraz reagowania na incydenty komputerowe przez wymianę informacji, tworzenie procedur działania i ćwiczenia wspólnie z zaufanymi partnerami.

W zakresie tworzenia i egzekwowania prawa dotyczącego cyberprze-

strzeni, USA chcą ustanowić partnerstwa z krajowymi organami ścigania, rozpocząć międzynarodową dyskusję na temat rozwoju nowych norm prawnych, a także harmonizować istniejące normy krajowe i usprawnić przestrzeganie obowiązujących norm i konwencji międzynarodowych (ze szczególnym uwzględnieniem konwencji z Budapesztu). Zdaniem autorów strategii, należy koncentrować się przede wszystkim na działaniach prewencyjnych i skutecznym karaniu winnych przestępstw w cyberprzestrzeni. Działaniom tym nie powinna jednak towarzyszyć kampania szerokiego ograniczania dostępu do Internetu, gdyż jej ofiarami bywają niewinni użytkownicy sieci. Tworzone prawo powinno także stwarzać warunki pozwalające na skuteczne ograniczanie dostępu do sieci osób wykorzystujących ją do prowadzenia nielegalnej działalności.

Podstawą działań sił zbrojnych w zakresie obrony cyberprzestrzeni ma być podnoszenie zdolności do operowania w tym środowisku, a także tworzenie i zacieśnianie sojuszy wojskowych w celu budowy potencjału do wspólnego przeciwstawienia się zagrożeniom w sieci. Współpraca ma obejmować budowę wspólnych systemów ostrzegania i wymiany informacji oraz rozwijanie zdolności do współdziałania zarówno w czasie pokoju, jak i w sytuacjach kryzysowych. Szczególnie istotną kwestią będzie tworzenie mechanizmów kolektywnej obrony w cyberprzestrzeni i tworzenie planów ewentualnościowych, pozwalających na izolowanie zagrożenia, ograniczenie jego skutków oraz zablokowanie efektu domina.

Stany Zjednoczone podkreślają prawo każdego państwa do samoobrony. Zgodnie z nową strategią, USA będą reagowały na niebezpieczeństwo w cyberprzestrzeni wykorzystując wszelkie niezbędne środki – dyplomatyczne, informacyjne, militarne i ekonomiczne – dozwolone przez prawo międzynarodowe. Rozwiązania militarne pozostaną jednak ostatecznością, po którą USA sięgną dopiero po wyczerpaniu wszystkich innych środków.

Proponowane przez Stany Zjednoczone rozwiązania w zakresie obrony cyberprzestrzeni są zgodne z zapisami Koncepcji Strategicznej NATO, podpisanej w 2010 r. w Lizbonie[5]. Można oczekiwać, że w sprawach współpracy wojskowej przy rozwijaniu zdolności obronnych w cyberprzestrzeni USA będą dążyły w pierwszej kolejności do tworzenia bliższych partnerstw z krajami członkowskimi Sojuszu Północnoatlantyckiego. Przemawia za tym także fakt, że znaczna część ataków w sieci przeprowadzana jest z terytorium państw nienależących do Sojuszu, głównie Rosji i Chin[6].

---

[5] *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*, 19-20 listopada 2010 r., http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (dostęp: 26 maja 2011 r.).

[6] J. Ryancia, *CIA Director Leon Panetta warns of possible cyber-Pearl Harbor*, ABC News, 11 lutego 2011 r., http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905 (dostęp: 26 maja 2011 r.).

NOWA STRATEGIA W PRAKTYCE[7]

Kilkanaście dni po opublikowaniu amerykańskiej strategii dotyczącej cyberprzestrzeni pojawiły się pierwsze informacje o jej praktycznym zastosowaniu przez władze USA. Według informacji medialnych[8], Departament Obrony USA pracuje nad własną strategią, zgodnie z którą Stany Zjednoczone będą miały prawo zinterpretować incydent komputerowy, spowodowany przez inne państwo, jako działanie wojenne. Przewiduje się, że liczący ok. 30 stron (w tym 12 stron jawnych) dokument sam w sobie będzie elementem systemu odstraszania potencjalnych adwersarzy. Zgodnie z wstępnymi informacjami, władze Stanów Zjednoczonych pracują obecnie nad szczegółami mającymi precyzować, jaki rodzaj ataku będzie konstytuował użycie konwencjonalnych sił zbrojnych w reakcji na atak przeprowadzony w lub przy użyciu cyberprzestrzeni. USA traktują cyberprzestrzeń jako kolejne pole walki (obok lądu, morza i powietrza). Ich zdaniem w odniesieniu do przestrzeni wirtualnej należy stosować te same zasady prawa międzynarodowego, co do „tradycyjnych" działań wojennych. Zachowana miałaby być zasada „równoważności" (*equivalence*) działań odwetowych. Przykładowo, jeśli cyberatak na element infrastruktury krytycznej USA spowodowałby wymierne szkody fizyczne (odcięcie energii elektrycznej, zniszczenie systemu bankowego itp.), śmierć amerykańskich obywateli lub wysoki poziom zakłóceń funkcjonowania kraju, Stany Zjednoczone miałyby prawo do odpowiedzi na taki akt za pomocą adekwatnych środków – również militarnych. Działania te będą jednak przypuszczalnie podejmowane tylko w sytuacji, gdy za atakiem będzie stało inne państwo, osoba lub osoby działające na zlecenie państwa. Nowa strategia Pentagonu prawdopodobnie nie będzie dotyczyła ataków przeprowadzanych przez aktorów niepaństwowych – przestępców i terrorystów, a przynajmniej nie będzie dopuszczała w tym kontekście stosowania reguły „równoważności".

Ponieważ istniejące dokumenty regulujące międzynarodowe prawo konfliktów zbrojnych nie przewidują możliwości prowadzenia wojny w cyberprzestrzeni, USA mają przeprowadzić konsultacje z sojusznikami, których celem będzie wypracowanie wspólnej interpretacji tych dokumentów, tak aby można było je stosować w odniesieniu do wojen w sieci. Stany Zjednoczone chcą też skłonić partnerów do synchronizacji doktryn militarnych w celu lepszej koordynacji

[7] 14 lipca 2011 r. Departament Obrony USA opublikował jawną wersję strategii działania w cyberprzestrzeni (Department of Defense Strategy for Operating in Cyberspace). Jednak wbrew informacjom mediów, strategia ta nie mówi o militarnych działaniach odwetowych za ataki na USA przeprowadzone w cyberprzestrzeni. Dokument opisuje pięć inicjatyw strategicznych Departamentu Obrony, które opierają się raczej na „miękkich" działaniach w dziedzinie cyberbezpieczeństwa (m.in. na zmianach proceduralnych i organizacyjnych, współpracy krajowej i międzynarodowej oraz rozwoju technologii służącej bezpieczeństwu cyberprzestrzeni). Można przypuszczać, że zagadnienia związane z aspektami militarnymi i działaniami odwetowymi zostały zawarte w niejawnej wersji strategii; *Lynn: Cyber Strategy's Thrust is Defensive,* U.S. Department of Defense, 14 lipca 2011 r., http://www.defense.gov/news/newsarticle.aspx?id=64682 (dostęp: 20 lipca 2011 r.).

[8] S. Gorman, Cyber combat: act of war, „The Wall Street Journal", 31 maja 2011 r., http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html# (dostęp: 5 czerwca 2011 r.).

działań i współpracy w zakresie obrony cyberprzestrzeni.

Mimo że nowy dokument jest dopiero opracowywany, już teraz budzi kontrowersje i pytania. Jeśli strategia ma okazać się skuteczna w praktyce, Stany Zjednoczone będą musiały znaleźć na nie przekonujące odpowiedzi. Największe wątpliwości związane są z możliwością precyzyjnego określenia agresora odpowiedzialnego za przeprowadzenie ataku. Dotychczasowe doświadczenia pokazują, że szybkie i dokładne określenie miejsca, z którego faktycznie nastąpił atak, jest trudne. Nawet jeśli uda się tego dokonać, wskazane zostanie jedynie fizyczne położenie komputera, nie uzyska się natomiast odpowiedzi na pytania, kto był jego operatorem, kto napisał jego oprogramowanie i czy jego działania są motywowane przez państwo. Przypadki zmasowanych cyberataków na Estonię w 2007 r. czy Gruzję w 2008 r. są często łączone z Rosją, jednak mimo upływu czasu nie udało się wskazać bezpośrednich związków między tymi atakami a państwem rosyjskim. Za wielokrotne ataki na serwery firmy Google obarcza się odpowiedzialnością Chiny[9]. Nie jest to jednak do końca oczywiste, a USA poprosiły o pomoc w prowadzeniu śledztwa stronę chińską, oskarżaną przez amerykańską korporację.

Stany Zjednoczone deklarują, że odpowiedź na wrogie działanie będzie adekwatna do wyrządzonych szkód, a wykorzystanie konwencjonalnych środków militarnych będzie ostatecznością, braną pod uwagę po wyczerpaniu narzędzi politycznych i ekonomicznych. Nie jest jednak jasne, w jaki sposób USA będą oceniały skutki ataków pod kątem wyboru adekwatnej na nie reakcji[10]. Nie wiadomo również, jak Stany Zjednoczone będą reagowały na agresywne działania w cyberprzestrzeni podejmowane przeciw wrogom Ameryki przez kraje sojusznicze, niezwiązane formalnie zasadami strategii opracowywanej przez Pentagon. Niejasne jest też, jak do nowej strategii będą stosowały się same Stany Zjednoczone, które otwarcie przyznają się do rozwijania swojego potencjału cybernetycznych środków walki[11] oraz są podejrzewane m.in. o udział w sabotowaniu irańskiego programu nuklearnego przy pomocy robaka Stuxnet[12].

Inicjatywa podejmowana przez Stany Zjednoczone jest istotnym pierwszym krokiem ku poprawie bezpieczeństwa globalnej sieci. Wydaje się jednak, że lepszym i skuteczniejszym rozwiązaniem niż swobodna interpretacja istniejącego prawa międzynarodowego przez jedno państwo byłoby stworzenie nowe-

---

9 *USA podniosły wobec Chin kwestię hakerskiego ataku na Google'a*, PAP z 3 czerwca 2011 r., http://stooq.pl/n/?f=469720&c=1&p=0 (dostęp: 7 czerwca 2011 r.).

10 Podobne wątpliwości pojawiły się w przypadku Koncepcji Strategicznej NATO z 19–20 listopada 2010 r. i oceny możliwości zastosowania Art. 5 Traktatu Waszyngtońskiego w odniesieniu do ataków cybernetycznych.

11 E. Nakashima, *List of cyber-weapons developed by Pentagon to streamline computer warfare*, „The Washington Post", 1 czerwca 2011 r., http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html (dostęp: 7 czerwca 2011 r.).

12 Ch. Williams, *Stuxnet virus: US refuses to deny involvement*, „The Telegraph", 27 maja 2011 r., http://www.telegraph.co.uk/technology/news/8541587/Stuxnet-virus-US-refuses-to-deny-involvement.html (dostęp: 7 czerwca 2011 r.).

go dokumentu, który wprowadziłby globalne reguły dotyczące bezpieczeństwa cyberprzestrzeni, wypracowane w drodze konsultacji międzypaństwowych.

Informacje dotyczące opracowywanej przez Departament Obrony USA strategii pochodzą z wiadomości prasowych, dlatego z ostateczną oceną dokumentu należy poczekać do momentu jego publikacji. Obecnie wydaje się jednak, że będzie ona miała raczej wąskie zastosowanie, a jej wymiar pozostanie symboliczny. W zakresie bezpieczeństwa cyberprzestrzeni dużo bardziej zasadne i motywowane względami praktycznymi wydaje się przygotowanie doktryny dotyczącej przeciwdziałania i zwalczania nielegalnej aktywności aktorów niepaństwowych – anonimowych użytkowników sieci, grup hakerów, przestępców oraz terrorystów wykorzystującymi Internet do realizowania swoich celów. Działania tego typu są bardziej powszechne i częściej dotykają zwykłych użytkowników sieci. Biorąc pod uwagę sposób funkcjonowania cyberprzestrzeni i jej użytkowników, można przyjąć, że ewentualne cyberkonflikty będą przypominały raczej wojnę partyzancką niż regularne starcia wrogich armii.

CO NOWA STRATEGIA MOŻE OZNACZAĆ DLA POLSKI

Amerykańska propozycja międzynarodowej współpracy w zakresie rozwoju cyberprzestrzeni może być okazją do wykorzystania potencjału, jakim dysponuje Polska. Strategiczne partnerstwo ze Stanami Zjednoczonymi powinno zostać wykorzystane do rozwijania współpracy z amerykańskimi partnerami, zarówno na poziomie najwyższych władz państwowych, instytucji rządowych zajmujących się cyberprzestrzenią, jak i przez polskie podmioty prywatne.

USA chcą budować partnerstwa z możliwie największą liczbą państw, organizacji i przedsiębiorstw. Dlatego też angażując się w początkową fazę powyższej inicjatywy, Polska miałaby szansę uczestniczenia w jej rozwoju i stać się niejako „ambasadorem" przedsięwzięcia np. na forum Unii Europejskiej czy wśród państw regionu Europy Środkowo-Wschodniej. Obecność Polski w tym projekcie – w związku z jego rozproszonym i ponadkrajowym charakterem – wydaje się konieczna. Polska nie może działać w oderwaniu od „głównego nurtu" rozwoju cyberprzestrzeni.

Często zwraca się uwagę, że rozwiązania dotyczące bezpieczeństwa cyberprzestrzeni w Polsce tworzone są w sposób nieskoordynowany, z wyraźnym podziałem zadań realizowanych przez poszczególne instytucje, których współpraca bywa utrudniona przez brak odpowiednich norm prawnych. Rozwiązaniem tego problemu mogłoby być powołanie centralnego ośrodka, którego zadaniem byłoby koordynowanie tych przedsięwzięć na szczeblu krajowym. Wprawdzie tworzone są dokumenty strategiczne dotyczące zagadnień związanych z bezpieczeństwem cyberprzestrzeni, jednak praktyczne działania w tym zakresie często mają charakter wyłącznie reaktywny. Tworząc nowe instytucje, podejmując decyzje organizacyjne czy wreszcie opracowując nowe prawo, polscy decydenci powinni unikać „uczenia się" na własnych błędach. Powinni natomiast korzystać z doświadczeń innych państw, aby nie

powielać popełnionych przez nie w przeszłości pomyłek. Z tego względu zalecane jest dążenie do wymiany informacji i doświadczeń na forum międzynarodowym oraz uczestniczenie w organizowanych ćwiczeniach – zarówno wojskowych, jak i cywilnych. W miarę możliwości należy również konsultować decyzje podejmowane w obszarze rozwoju i obrony cyberprzestrzeni, a także jej fizycznej infrastruktury, w tym decyzje z zakresu prawa do wolnej wymiany informacji w Internecie, wolności słowa, prawa do prywatności i ochrony danych użytkowników sieci.

Polska dysponuje bogatym kapitałem intelektualnym, który mógłby zostać wykorzystany jako wkład w rozwój globalnej sieci. Polscy informatycy od lat wygrywają międzynarodowe zawody i stali się uznanymi na świecie specjalistami. Minister gospodarki Waldemar Pawlak informował, że zgodnie z decyzją polskiego rządu, w najbliższych latach informatyka będzie traktowana jako sektor strategiczny. Na tegorocznych targach komputerowych CeBIT, Ministerstwo Gospodarki zorganizowało dwa stoiska narodowe pod hasłami „Invest in Poland" oraz „Informatyka Polską Specjalnością"[13].

Niezależnie od tego, jaka będzie decyzja polityczna dotycząca zaangażowania Polski w inicjowany przez Stany Zjednoczone projekt, powinna ona zostać poprzedzona spotkaniami z przedstawicielami USA, podczas których wyjaśnią oni szczegóły planowanych przedsięwzięć oraz wskażą obszary współpracy z sojusznikami zapraszanymi do realizacji celów nowej strategii. Polska, dysponując ograniczonymi środkami materialnymi (np. militarnymi), ma szansę wykorzystać swój bogaty potencjał intelektualny, aby działać na nowym polu współpracy i praktycznie wpływać na realizację strategii. Przedstawiciele polskich instytucji publicznych, ośrodków akademickich i sektora prywatnego mogą zaoferować wkład w rozwój projektu i wymianę doświadczeń z zagranicznymi partnerami. Należy monitorować rozwój tej inicjatywy oraz wypracowywanych w jej ramach mechanizmów i rozwiązań.

[13] *Polska na CeBIT 2011*, Ministerstwo Gospodarki, http://www.mg.gov.pl/node/12862 (dostęp: 24 maja 2011 r.).