FAE Policy Paper
nr 27/2013

Andrzej KOZŁOWSKI

Afera Snowdena a cyberbezpieczeństwo USA

Jednym z najgorętszych tematów ostatnich miesięcy pozostaje afera związana z ujawnieniem przez Edwarda Snowdena szpiegowskich poczynań w cyberprzestrzeni Agencji Bezpieczeństwa Narodowego (NSA) Stanów Zjednoczonych. Snowden dla jednych bardzo szybko stał się bohaterem, dla drugich synonimem zdrajcy. Batalia między jego zwolennikami a przeciwnikami będzie się jeszcze toczyć przez długi czas. Zdecydowanie ważniejszym aspektem jego działalności jest jednak wpływ na bezpieczeństwo Stanów Zjednoczonych, a w szczególności na aspekt cyberbezpieczeństwa.

Cyberbezpieczeństwo priorytetem dla administracji Baracka Obamy

Dochodząc do władzy w 2009 r. Barack Obama ogłosił cyberbezpieczeństwo jednym z głównych priorytetów swojej polityki bezpieczeństwa. Z tą polityczną deklaracją wiązały się konkretne działania. Biały Dom opublikował w 2011 r. międzynarodową strategię działań w cyberprzestrzeni, Pentagon ujawnił część swojej strategii działania w cyberprzestrzeni, powołano również osobne Dowództwo Cybernetyczne (USCYBERCOM) podporządkowane Dowództwu Strategicznemu. Administracja B. Obamy podjęła również próby uchwalenia aktu prawnego, regulującego wymianę informacji między sektorem publicznym a prywatnym w celu szybszego informowania o potencjalnych zagrożeniach.

Jednym z ważniejszych punktów planowanych zmian miało być zaostrzenie kontroli przepływu danych wewnątrz instytucji. Szczególny nacisk na tę kwestię został położony po ujawnieniu przez amerykańskiego wojskowego Bradleya Manninga dużej ilości tajnych informacji portalowi Wikileaks. Jak się okazało nie miał on żadnych problemów ze skopiowaniem tajnych danych na własnego pendrive'a i wyniesieniem ich na zewnątrz. Po tym incydencie generał Keith B. Alexander, stojący na czele NSA i USCYBERCOM, wielokrotnie zapowiadał stworzenie skutecznego systemu zabezpieczającego wrażliwe informacje przed dostępem nieuprawnionych osób.

W czerwcu 2013 r. okazało się jednak, że zapowiadane zabezpieczenia nie zdały egzaminu. Edward Snowden, były pracownik CIA i firmy Booz Allen Hamilton – jednego z podwykonawców NSA – ujawnił na łamach brytyjskiej gazety „The Guardian" tajne informacje, które zaszokowały opinię publiczną na całym świecie. Snowden poinformował o istnieniu tajnego programu PRISM, dzięki któremu rząd Stanów Zjednoczonych ma dostęp do danych

gromadzonych na serwerach największych firm internetowych takich jak: Apple, Microsoft, Microsoft ze Skypem, Yahoo, Google wraz z YouTube'em, Facebook, PalTalk (komunikator sieciowy), AOL. Równie szokującą wiadomością było to, że przedsiębiorstwa te przystąpiły do tego programu dobrowolnie.

Informacje ujawnione przez Snowdena mają niewątpliwy wpływ na politykę bezpieczeństwa Stanów Zjednoczonych w cyberprzestrzeni, oddziałując na wewnętrzne mechanizmy zapewnienia cyberobrony, jak również na aktywność amerykańskiej cyberdyplomacji na arenie międzynarodowej.

Snowdengate a problem cyberbezpieczeństwa wewnątrz Stanów Zjednoczonych

Jednym z istotnych elementów cyberbezpieczeństwa każdego kraju jest społeczeństwo, które rozważnie używa Internetu, unikając potencjalnych zagrożeń i pułapek czyhających na nie, stając się pierwszą linią cyberobrony. Taki stan rzeczy może być osiągnięty jedynie przy kooperacji z rządem, który prowadząc rozsądną politykę edukacyjną informuje obywateli o potencjalnym złośliwym oprogramowaniu oraz innych przejawach szkodliwej działalności hakerów w sieci. Niezwykle ważne jest tutaj wzajemne zaufanie – społeczeństwo musi wierzyć, że instytucje rządowe faktycznie zamierzają pomóc w zapewnieniu bezpieczeństwa, a nie podejmują działania w celu szpiegowania i inwigilowania obywateli. Ujawnienie przez Snowdena informacji o szpiegowaniu w sieci zaszokowało Amerykanów i podważyło ich zaufanie do rządu. Został obalony mit Internetu jako przestrzeni wolnego i nieskrępowanego wyrażania myśli, i po raz kolejny powróciło pytanie odnośnie odpowiedniej proporcji między bezpieczeństwem a wolnością. *Snowdengate* spowodowała wzrost liczby zwolenników drugiej opcji, co nie może pozostać bez wpływu na próby ulepszenia i usprawnienia cyberobrony.

Widoczne są już pierwsze skutki ujawnienia przez Edwarda Snowdena informacji na temat programu PRISM. Jedną z istotnych reform, która miała zostać wdrożona w najbliższej przyszłości, było objęcie amerykańskich sieci prywatnych nadzorem programu EINSTEIN 3. Jest to oprogramowanie stosowane w sieciach instytucji państwowych USA. Jego głównym zadaniem jest monitorowanie przepływu danych pod kątem złośliwego oprogramowania i w razie konieczności ich przechwytywanie i neutralizowanie, zanim zdążą wyrządzić szkody. Mechanika działania tego instrumentu przypomina kontrowersyjny PRISM. Biorąc pod uwagę ogólną

panikę, która zapanowała w Stanach Zjednoczonych po ujawnieniu działań NSA, wdrożenie takiego rozwiązania nie może się udać, ponieważ napotkałoby to na poważny opór ze strony społeczeństwa. W opinii Amerykanów nie stanowiłoby to próby zapewnienia bezpieczeństwa, ale byłoby to wprowadzeniem kolejnej metody inwigilacji. Przy obecnej sytuacji dla większości społeczeństwa, o wiele większym zagrożeniem wydaje się sama NSA niż cyberprzestępcy, cyberszpiedzy czy inna szkodliwa działalność w sieci. Niestety, żeby zmienić to nastawienie i wprowadzić zakładane reformy, być może konieczne będzie inne szokujące wydarzenie, np. w postaci „cybernetycznego Pearl Harbour", czy ataków na skalę tych z 11 września 2001 r. Brak objęcia nadzorem przez EINSTEIN 3 sieci prywatnych prowadziło będzie do większego narażenia amerykańskich przedsiębiorstw na ataki hakerskie, co w konsekwencji przyniesie im jeszcze większe straty finansowe, niż dotychczas.

Ujawnienie przez E. Snowdena rewelacji dotyczących amerykańskie cyberobrony będzie miało też wpływ na toczący się w Kongresie proces tworzenia prawa, które umożliwiłoby szybką wymianę informacji na temat zagrożeń w środowisku wirtualnym pomiędzy sektorem prywatnym a publicznym. Obecnie na Kapitolu trwają dyskusje nad Cyber Intelligence Sharing and Protection Act (CISPA), ustawą która miałaby wcielić tą idee w życie. Afera Snowdena zbiegła się w czasie z przekazaniem CISPY pod obrady w Senacie. Spodziewano się uchwalenia poprawek i przekazania dokumentu do ponownego rozpatrzenia do Izby Reprezentantów. Obecnie jednak CISPA jest postrzegana powszechnie jako kolejny krok ku szpiegowaniu Amerykanów, a nie zapewnieniu bezpieczeństwa amerykańskim przedsiębiorcom i jej los wydaje się przesądzony.

Snowdengate nie dotknie jednak tylko CISPY, ale również innych aktów prawnych, których celem miałoby być rozwiązanie tego problemu w przyszłości. Będą one pod wnikliwą obserwacją mediów i różnych organizacji broniących wolności w Internecie, przez co politycy mogą pójść na kompromis i zamiast postawić ma skuteczną cyberobronę, wybiorą mniej ograniczające wolność, ale zarazem i mniej skuteczne rozwiązania.

Snowdengate może nie tylko wpłynąć na przyszłe ustawodawstwo Kongresu dotyczące wymiany informacji pomiędzy sektorem publicznym a prywatnym, ale także na istniejące już prawo, regulujące kompetencje agencji odpowiedzialnych za cyberbezpieczeństwo Stanów Zjednoczonych. Republikanin Justin Amash zaproponował poprawkę, która miałaby zabronić

NSA gromadzenia i przechowywania informacji uzyskanych przez podsłuchiwanie rozmów telefonicznych. Minimalną ilością głosów została ona odrzucona. Inny republikański kongresmen Rush Holt zasugerował wprowadzenie zmian w Patriotic Act i Foreign Intelligence Surveillance Act, które zmniejszałyby możliwości inwigilowania obywateli ze strony rządu. Jego propozycja nie spotkała się jednak z wystarczającym poparciem. W przyszłości mogą się pojawiać podobne wnioski, a ich los nie jest wcale z góry przesądzony.

Ujawnienie informacji przez E. Snowdena pokazuje również, że mimo zapowiedzi, system kontrolowania przepływu informacji wewnątrz instytucji państwowych pozostawia wiele do życzenia. Widać, że zapowiadane reformy po incydencie z B. Manningem nie sprawdziły się i wiele pozostaje do zrobienia w tej kwestii. Inną kontrowersyjną sprawą, która powinna ulec zmianie, jest możliwość dostępu do tajnych danych przez pracowników firm – podwykonawców. E. Snowden nie był przecież nigdy pracownikiem NSA, a przeglądał wrażliwe dla bezpieczeństwa państwa informacje. Stany Zjednoczone, jeśli chcą w przyszłości uniknąć przypadków podobnych do afer Snowdena i Manninga, muszą rozwiązać ten problem.

Problem związany z ujawnieniem informacji przez byłego pracownika CIA może skomplikować rekrutację tzw. etycznych hakerów, którzy chcą swoją wiedzę wykorzystać w imię dobra państwa. Snowdengate prowadzić może do sytuacji, że wielu z nich nie zostanie zatrudnionych, ponieważ będzie zachodziła obawa, że mogą oni stać się źródłem kolejnego przecieku.

Snowdengate, w opinii niektórych, nie przyniesie wyłącznie negatywnych skutków, a wręcz przeciwnie – może przyczynić się do poprawy niektórych elementów cyberbezpieczeństwa. Zdanie to podziela James Clapper, dyrektor amerykańskiego wywiadu państwowego, który postrzega *Snowdengate* jako bodziec pobudzający debatę publiczną na temat odpowiedniego zbalansowania prawa do prywatności i bezpieczeństwa narodowego. Jego zdaniem większa otwartość ze strony służb wywiadowczych spowoduje, że wzrośnie do nich zaufanie obywateli. Wypowiedzi Clappera powinny być jednak interpretowane jako robienie dobrej miny do złej gry, ponieważ Stany Zjednoczone już zapłaciły wysoką cenę za transparentność działania wywiadu i fakt, że zbyt duża liczba osób ma możliwość wejścia w posiadanie kluczowych dla bezpieczeństwa państwa danych. Jednakże, faktycznym pozytywnym skutkiem ujawnienia przez Snowdena informacji, może być zaostrzenie procedur bezpieczeństwa

w amerykańskim sektorze prywatnym. Przedsiębiorstwa w obawie przed szpiegostwem ze strony swojego rządu mogą wprowadzić dodatkowe zabezpieczenia, która utrudnią infiltrację ich sieci. Obecnie przyjmuje się, że 2/3 amerykańskich firm zostało zhackowanych, z czego duża część z nich dowiaduje się o tym po fakcie, albo dostrzega to bardzo późno.

Trudne wyzwanie na arenie międzynarodowej

Szkodliwość *Snowdengate* na sytuację cyberbezpieczeństwa wewnątrz USA jest aż nadto widoczna. O wiele gorsze mogą się jednak okazać następstwa na arenie międzynarodowej, które zaszkodzą amerykańskiemu cyberbezpieczeństwu.

Ujawnienie informacji przez E. Snowdena zdyskredytowało Stany Zjednoczone w oczach ich sojuszników. Upublicznione przez byłego pracownika CIA dane pokazały wprost, że Amerykanie szpiegują swoich sprzymierzeńców. Poza głosami oburzenia płynącymi z całego świata, niektóre państwa podjęły konkretne działania. Niemcy zerwały umowę z lat 60. XX wieku, podstawie której Stany Zjednoczone, Wielka Brytania i Francja miały dostęp do wyników nasłuchu prowadzonego przez zachodnioniemiecki wywiad zagraniczny BND oraz Urząd Ochrony Konstytucji w zakresie dotyczącym bezpieczeństwa amerykańskich i brytyjskich wojsk stacjonujących w Niemczech. Rząd w Berlinie wypowiedział tę umowę, jako powód wskazując fakt, że dalsza współpraca z NSA może narazić na szwank prywatność niemieckich obywateli.

Niepokój sojuszniczych wywiadów wzbudza też słabe zabezpieczenie informacji o współpracy przez Amerykanów. Brytyjskie The Government Communications Headquarters (GCHQ) znalazło się w ogniu miażdżącej krytyki ze strony mediów za bliską kooperację z NSA. W zapewnieniu cyberbezpieczństwa bardzo istotnym jest współpraca z sojusznikami i dzielenie się z nimi informacjami. Sytuacja, w której Amerykanie nie są w stanie skutecznie zabezpieczyć danych o kooperacji wywiadowczej z innymi państwami, powoduje utratę wiarygodności. Może to prowadzić do zmniejszenia intensywności wymiany informacji, a część państw całkowicie zniechęcić do współpracy.

Największy wpływ Snowdengate można zauważyć w relacjach amerykańsko-chińskich w cyberprzestrzeni. Na początku XXI wieku chińscy hakerzy rozpoczęli zmasowaną kampanię cyberszpiegowską, wymierzoną w amerykańskie przedsiębiorstwa i instytucje państwowe. Zdobyte dane miały ułatwić i przyspieszyć rozwój chińskiej gospodarki i sił zbrojnych. W latach

2003–2005 trwała operacja Titan Rain, w wyniku której wykradziono wiele cennych danych m.in. plany F-35. W następnych latach Chińczycy również nie dawali o sobie zapomnieć, przeprowadzając kolejne operacje cyberszpiegowskie, wykradając dalsze informacje na temat projektów zbrojeniowych. Stany Zjednoczone dość biernie odnosiły się do tego zjawiska, potępiając cybeszpiegostwo, ale nie wskazując wprost na głównego winowajcę. Zmiana nastąpiła w 2013 r., kiedy to amerykańska firma Mediant zajmująca się bezpieczeństwem teleinformatycznym opublikowała raport, w którym wskazała, że chińska jednostka wojskowa 61398 jest odpowiedzialna za wiele aktów cyberszpiegostwa na amerykańskim terytorium. W jego następstwie Departament Stanu i Departament Obrony wzmocniły naciski na stronę chińską, publicznie oskarżając rząd w Pekinie o szpiegowanie w cyberprzestrzeni.

Szczyt USA-Chiny w czerwcu 2013 r. był pierwszym spotkaniem amerykańskiego prezydenta i nowo wybranego chińskiego przywódcy Xi Jinping. Wśród wielu tematów rozmów jednym z najważniejszych miało być cyberszpiegostwo. Obama planował zademonstrować dowody pokazujące skalę i skutki chińskiego działania. Tak się jednak nie stało, a to za sprawą ujawnionych przez Snowdena – tuż przed rozpoczęciem spotkania przywódców – informacji na temat szpiegowania w przestrzeni wirtualnej przez Amerykanów. Chińczycy od dawna oskarżali o te praktyki rząd w Waszyngtonie, ale nie posiadali przekonywujących dowodów. Zostały one im dostarczone w momencie opublikowania przez The Guardian rewelacji Snowdena. W takiej atmosferze poruszanie przez prezydenta Obamę kwestii cyberszpiegostwa byłoby hipokryzją i pozbawione jakiekolwiek wiarygodności. Zamiast krytyki Chin, to Stany Zjednoczone stały się główną ofiarą mediów, w tym chińskich, które bardzo ostro zaatakowały Amerykanów.

Ujawnienie przez Snowdena informacji nie tylko wpłynęło na szczyt Obama-Jinping, ale skomplikowało relacje chińsko-amerykańskie w cyberprzestrzeni. Przed długi okres czasu to chińscy hakerzy byli postrzegani jako napastnicy, a Amerykanie tylko i wyłącznie jako ofiary. Ten prosty dwuwymiarowy obraz sytuacji uległ teraz zmianie. Z drugiej jednak strony zmiana sytuacji w cyberprzestrzeni może zaowocować bliższą współpracą między oboma krajami, gdzie Chiny nie będą występowały już w roli agresora, ale będą postrzegane tak samo jak Stany Zjednoczone, jako napastnik i ofiara. Co więcej, Amerykanie zamiast skupiać się na krytykowaniu działalności Chińczyków, mogą włożyć więcej wysiłku w osiągniecie porozumienia.

Inną problematyczną kwestią w przypadku relacji tych państw w cyberprzestrzeni była rywalizacja ideologiczna. Stany Zjednoczone optowały za nieskrepowaną wolnością Internetu, kontrolowanego przez prywatne przedsiębiorstwa. Rządzący w Waszyngtonie przeciwstawiali się jakiekolwiek kontroli Internetu przez międzynarodowe organizacje. Chiny stały na przeciwległym biegunie, twierdząc, że kluczem do zapewnienia bezpieczeństwa w cyberprzestrzeni jest rygorystyczna kontrola Internetu przez państwowe i międzynarodowe instytucje. W tej ideologicznej batalii Amerykanie jawili się jako obrońcy wolności i demokracji. *Snowdengate* pokazała, że była to jedna wielka hipokryzja. Stany Zjednoczone czerpały korzyści z Internetu, kontrolowanego przez prywatne, głównie amerykańskie przedsiębiorstwa, mając dostęp do przechowywanych przez nie informacji. Może to doprowadzić do sytuacji, że np. państwa afrykańskie przyjmą chiński model w Internecie i dołączą do Chin w jego promocji na forum ONZ, co zaszkodzi amerykańskim interesom w cyberprzestrzeni.

Zakończenie

Afera związana z ujawnieniem przez Edwarda Snowdena informacji na temat inwigilacji w Internecie była jednym z najgłośniejszych wydarzeń na arenie międzynarodowej ostatnich miesięcy. Stanowi też najpoważniejszy przeciek informacji w historii Stanów Zjednoczonych i nie pozostanie bez wpływu na bezpieczeństwo, a w szczególności na cyberbezpieczeństwo tego państwa. *Snowdengate* zdecydowanie przyczyniła się do osłabienia amerykańskiej cyberobrony, wpływając negatywnie na wewnętrzne próby jej wzmocnienia w Stanach Zjednoczonych, jak również na wysiłki podejmowane w tym celu na arenie międzynarodowej. Informacje ujawnione przez Snowdena odsłoniły całą strukturę pozyskiwania danych przez amerykański wywiad w Internecie. Przedsiębiorstwa i sojusznicy, którzy jeszcze niedawno dzieli się informacjami na temat zagrożeń, mogą zredukować obecnie stopień i zakres współpracy. Bez odpowiednich informacji niezmiernie trudno będzie tymczasem zapobiegać cyberatakom, na czym ucierpi zarówno rząd, jak i przedsiębiorstwa USA – a w konsekwencji amerykańscy obywatele.

Kontakt

**Fundacja
Aleksandra Kwaśniewskiego
„Amicus Europae”**

Aleja Przyjaciół 8/5
00-565 Warszawa

Tel. +48 22 622 66 33
Tel. +48 22 622 66 03
Fax:+48 22 629 48 16

email: fundacja@fae.pl, www.fae.pl

FAE Policy Paper nr 27/2013

**Afera Snowdena
a cyberbezpieczeństwo USA**

Autor: Andrzej Kozłowski

Ekspert Instytutu Kościuszki. Członek redakcji pisma „Stosunki Międzynarodowe”. Doktorant na Wydziale Studiów Międzynarodowych i Politologicznych UŁ. W kręgu jego zainteresowań znajdują się cyberbezpieczeństwo, region Kaukazu Południowego oraz polityka bezpieczeństwa i zagraniczna USA

Nadrzędną misją **Fundacji AMICUS EUROPAE** jest popieranie integracji europejskiej, a także wspieranie procesów dialogu i pojednania, mających na celu rozwiązanie politycznych i regionalnych konfliktów w Europie.

Do najważniejszych celów Fundacji należą:

- Wspieranie wysiłków na rzecz budowy społeczeństwa obywatelskiego, państwa prawa i umocnienia wartości demokratycznych;
- Propagowanie dorobku politycznego i konstytucyjnego Rzeczypospolitej Polskiej;
- Propagowanie idei wspólnej Europy i upowszechnianie wiedzy o Unii Europejskiej;
- Rozwój Nowej Polityki Sąsiedztwa Unii Europejskiej, ze szczególnym uwzględnieniem Ukrainy i Białorusi;
- Wsparcie dla krajów aspirujących do członkostwa w organizacjach europejskich i euroatlantyckich;
- Promowanie współpracy ze Stanami Zjednoczonymi Ameryki, szczególnie w dziedzinie bezpieczeństwa międzynarodowego i rozwoju gospodarki światowej;
- Integracja mniejszości narodowych i religijnych w społeczności lokalne;
- Propagowanie wiedzy na temat wielonarodowej i kulturowej różnorodności oraz historii naszego kraju i regionu;
- Popularyzowanie idei olimpijskiej i sportu.