POLITYKA I STRATEGIA BEZPIECZEŃSTWA PAŃSTWA

Mgr Mariusz RZESZUTKO

HAKTYWIZM – CYFROWE OBLICZE WSPÓŁCZESNEJ SOLIDARNOŚCI, CZY ZAGROŻENIE BEZPIECZEŃSTWA WEWNĘTRZNEGO PAŃSTWA?

Wstęp

Każdego dnia nasze życie coraz bardziej uzależnione jest od Internetu i coraz częściej przenosimy je właśnie w tę sferę. Wirtualne zakupy, konta bankowe, odległe kontakty przy pomocy portali społecznościowych, rozmowy wykorzystujące technologię VoIP, elektroniczna komunikacja między rządami państw, w końcu elektroniczny nadzór nad bronią. Nie trudno zatem o refleksję, iż do świata tego przenoszą się także konflikty zbrojne oraz dyplomatyczne. W przeciwieństwie do tzw. „reala" – wirtualnie protestująca społeczność ma tutaj jednak równe, bądź nawet większe szanse niż strona rządów, organizacji międzynarodowych, czy wielkich korporacji.

Hacking + activism

Pojęcie haktywizmu jest neologizmem, zręczną grą słów – połączeniem hackerstwa oraz aktywizmu.

Stworzone i po raz pierwszy użyte przez *Omegę* – członka utworzonego w 1984 roku *Kultu Martwej Krowy* – grupy hakerów, którzy działając w imię wolności słowa dokonywali notorycznego łamania obowiązującego prawa[1].

Według Gabrielli Coleman z Katedry Kompetencji Naukowych i Technologicznych Uniwersytetu McGill w Stanach Zjednoczonych – to *świadczenie pomocy*

[1] http://news.cnet.com/8301-27080_3-57406793-245/old-time-hacktivists-anonymous-youve-crossed-the-line/.

technologicznej w imię obrony praw człowieka. Jednakże to także protesty, które naginają prawo, bądź bezpośrednio je łamią. Haktywizm dopuszcza także sabotaż w celu artykulacji własnych przekonań[2].

Według samego autora definicji – *If hacking as „illegally breaking into computers" is assumed, then hacktivism could be defined as „the use of legal and/or illegal digital tools in pursuit of political ends"* [tłum. autor: Jeżeli zakłada się, że hacking jest nielegalnym włamywaniem się do komputerów, haktywizm należy definiować jako użycie legalnych, bądź nielegalnych środków cyfrowych, w ramach realizacji celów politycznych.][3].

Haktywizm jest więc odmianą protestu, akcji oraz aktów nieposłuszeństwa obywatelskiego w wymiarze cyfrowym[4]. Poprzez podejmowane działania, haktywiści wirtualnie protestują przeciw określonym zjawiskom i wydarzeniom, a przyczyna ich wystąpień ma najczęściej wymiar polityczny lub ekonomiczny. Walczą o wolność, o prawo do własnego zdania, władzę dla narodu, swobodę protestu przeciw decyzjom władz, zniesienie cenzury.

Równie często działania te mają na celu także nagłośnienie problemu, bądź pozyskania jak największej ilości zwolenników akcji społecznych, religijnych, czy politycznych[5]. Pierwotny haktywizm był przejawem walki o wolność ludzi o niskiej tolerancji na kłamstwa władzy.

Termin ten, podobnie jak sam ruch wciąż ewoluuje i nie sposób określić jego ostatecznej definicji. Pierwsi haktywiści wykazywali się niezwykłą wiedzą, którą wykorzystywali zgodnie ze swoim sumieniem w imię walki o wolność. Dzisiejsza definicja cyfrowych aktywistów nie jest już tak oczywista i jednoznaczna. Współczesny haktywizm coraz częściej opiera się bowiem na działaniach technogeeków[6] – osób o dużych zdolnościach technologicznych, znajomości nowinek i urządzeń elektronicznych, świadomych możliwości jakie one niosą. W ostatnich latach za sprawą portalu 4chan.org – matki grupy ANONYMOUS, swój udział w haktywiźmie mogą mieć także zwykli użytkownicy, posiadający podstawową wiedzę w zakresie obsługi Internetu i komputera.

---

[2] Na przykład wirtualne strajki okupacyjne.

[3] http://www.abacuslaw.com/ps/2012/10/09/how-law-firms-can-combat-hacktivism/.

[4] http://webstyle.pl/netopedia/spoleczenstwo_informacyjne/haktywizm.

[5] Akcje religijne wymierzone były w kościół scientologiczny; ekonomiczne – w walkę z nieuczciwymi władzami oraz obywatelami; polityczne akcje miały na celu zdemaskowanie dyplomatycznych gier przy pomocy portalu WikiLeaks.

[6] http://www.urbandictionary.com/define.php?term=Technogeek.

Skomplikowane umiejętności włamywania się do systemów zastąpił więc dostęp do globalnej sieci, a zdolności programowania i bieżącego pokonywania zabezpieczeń – gotowe programy hackujące[7].

Dla władz państwowych, firmowych i religijnych, które padają najczęstszą ofiarą cybernetycznych aktywistów, pojęcie haktywizmu jest tożsame z hakerstwem, cyberprzestępczością a w skrajnych przypadkach – również cyberterroryzmem. Nie jest to jednak pojęcie tożsame. Różnice nie leżą jedynie w ideologii, lecz także organizacji oraz sposobie działania.

Poziom ideologiczny różniący haktywistów od internetowych przestępców, dotyczy pobudek aktywistów, którzy swoje akcje przeprowadzają dla dobra ogółu i takie też mają intencje. Cyberprzestępcy działają na rzecz własnego dobra, często posuwając się do kradzieży i wyrządzania krzywdy.

Celem haktywistów są najczęściej władze[8] nieskore do dialogu. Cyberprzestępców oraz cyberterrorystów zajmują z kolei ataki na ofiary cywilne, firmy, rzadziej organy władzy.

Także na poziomie organizacji zauważalne są realne różnice między obiema grupami. Haktywiści działają sposób chaotyczny, niezorganizowany i spontaniczny.

W przeciwieństwie do dobrze zorganizowanych i starających się ukryć swoje działania cyberprzestępców i cyberterrorystów – nie posiadają także przywódcy. Cybernetyczni aktywiści nie są zmuszani do uczestnictwa we wszystkich[9] podejmowanych protestach, nie tworzą także grupy o stałym składzie personalnym. Są więc swoistą merytokracją, opartą na szacunku przejściowego lidera, który organizując akcję odpowiada za jej koordynację. Po wypełnieniu misji ustępuje na rzecz innych haktywistów rozpoczynających własną akcję protestacyjną.

Ewolucja działalności

Pierwsze protesty haktywistów polegały na wysłaniu do odpowiedniej strony www, a więc bezpośrednio serwera, na którym była umieszczona, jednoczesnej takiej ilości wezwań tak, aby serwer nie był w stanie ich obsłużyć – doznając tym

[7] Na przykład stworzone przez hackerów Anonymous dla reszty zwykłych użytkowników 4chan.org tzw. Jonowe Działo Orbitalne – program, który wymagał jedynie wprowadzenia strony i wciśnięcia przycisku uruchom.

[8] To władze rządów, wielkich korporacji, a nawet przywódcy grup duchowych i sekt, czego egzemplifikacją była otwarta cybernetyczna wojna między ruchem Anonymous a sektą kościoła scientologicznego.

[9] Dzielą się wówczas na frakcje.

samym awarii, a co z tym związane – także zawieszenia żądanej witryny. Nieobce były im także tzw. emailowe ataki bombowe, polegające na spamowaniu[10] przez wielu użytkowników skrzynek mailowych organizacji, powodując tym samym ich całkowite zawieszenie[11].

Niezbyt chętnie potwierdzaną jawnie metodą, choć nader często stosowaną (także współcześnie), było również infekowanie przy pomocy wirusów i robaków systemów przeciwnika.

Pierwszą tego typu działalnością haktywistów było stworzenie i wpuszczenie w 1989 roku do DECNet'u robaka o nazwie WANK[12]. O ile nieszkodliwe oprogramowanie jako klasyczny przykład haktywizmu, przekazywało jedynie zdanie krytyki wobec nuklearnego wyścigu zbrojeń, nie wyrządzając żadnej szkody odbiorcy, o tyle kolejne robaki wypuszczane w latach 90. – atakowały, przechwytywały dane, a nawet niszczyły systemy przeciwnika.

We wrześniu 1998 roku grupa portugalskich hakerów przy pomocy złośliwego oprogramowania zmodyfikowała strony ponad 40 indonezyjskich serwerów, ustawiając w ich treści przesłanie społeczne – „Wolność dla Timoru Wschodniego". Z kolei w czerwcu tego samego roku grupa MilwOrm zmodyfikowała treść strony Indyjskiego Centrum Badania nad Atomem, ustawiając na stronie tytułowej hasło: „Jeśli nuklearna wojna się rozpocznie, będziecie pierwsi, którzy zaczną krzyczeć".

Niezwykle aktywny dla haktywistów rok 1998 przyniósł także atak grupy Legion of the Underground na strony Republiki Chińskiej. Do najsłynniejszych akcji tego roku należał również atak grupy Hacktivismo, której udało się zdezaktywować firewall założony przez komunistyczną władzę Chin. Dzięki temu chińscy użytkownicy Internetu mogli się cieszyć przez pewien czas niecenzurowanym dostępem do wszystkich stron internetowych świata. Było to pierwsze i ostatnie tak spektakularne naruszenie chińskich zabezpieczeń.

Jako ciekawostkę należy nadmienić, iż pierwsza wojna cybernetyczna wybuchła w Internecie pomiędzy Chinami a Tajwanem. Chińscy haktywiści atakujący tajwańskie serwery zmodyfikowali wówczas treść strony startowej, zamieniając ją na hasło *Tylko jedne Chiny istnieją i tylko jedne są potrzebne*.

---

[10] Wirtualny słownik języka polskiego określa spamowanie mianem wysyłania i rozpowszechniania niechcianych wiadomości elektronicznych, reklam oraz tzw. *łańcuszków*. W przypadku haktywistów konfliktu kosowskiego, każdy atakujący wysyłał setki listów obciążając serwery NATO.

[11] O tego typu ataku na NATO w czasie konfliktu w Kosowie poinformował rzecznik NATO Jamie Shea.

[12] Skrót oznaczał Worms Against Nuclear Killers, co w wolnym tłumaczeniu należy odczytywać jako Robaki Przeciwko Nuklearnym Mordercom.

30 marca 1999 roku w czasie trwania konfliktu kosowskiego belgradzcy hackerzy doprowadzili do całkowitego zawieszenia serwerów NATO[13].

Niezwykle popularnymi stały się także dokonywane pod koniec lat 90. internetowe protesty przeciw prezydentowi Meksyku – Zedillosowi, prezydentowi Clintonowi oraz światowym giełdom walutowym – wykorzystującym w opinii haktywistów zwykłych obywateli.

Typową akcją wymierzoną w rządy ograniczające prawa obywatelskie był *Jam Echelon Day* powołany w celu zniszczenia domniemanego Echelona – światowego systemu inwigilacji komunikacji cyfrowej. Dokładnie 21 października 1999 roku cybernetyczni działacze całego świata przy pomocy emailowych ataków bombowych zawierających w treści elektronicznych listów słowa o kluczowym znaczeniu dla systemu monitorującego, miały doprowadzić do jego przeciążenia, zawieszenia a nawet czasowego wyłączenia. Efekty akcji powtórzonej w 2000 roku pozostają do dziś wielką niewiadomą – podobnie jak istnienie samego systemu Echelon.

Jednym z najsłynniejszych ataków ostatnich lat było włamanie do Centrum Badania Zmian Klimatu im. Tyndalla przy University of East Anglia. Celem działaczy było zdobycie informacji obalających mit globalnego ocieplenia, który miał według włamywaczy służyć jedynie interesom naukowców. Zdobyta wówczas korespondencja pracowników naukowych próbujących zatuszować sprzeczne z szerzoną teorią wyniki badań potwierdzała podejrzenia hackerów, a jej upublicznienie wywołało poruszenie na arenie międzynarodowej.

Jedynie na przestrzeni lat 1989–2010, mieliśmy do czynienia z ponad 40 poważnymi, międzynarodowymi atakami haktywistycznymi[14].

Cybernetyczna wojna między haktywistami chińskimi i tajwańskimi przyczyniła się do rozwoju tego typu *cyfrowej polemiki* również między innymi zwaśnionymi krajami.

Eskalacja rosyjsko-estońskiego konfliktu dyplomatycznego z roku 2007, doprowadziła do wymazania przez rosyjskich crackerów[15] Estonii z internetowej mapy Europy. Podobny atak rosyjskich haktywistów na Litwę i Gruzję miał miej-

---

[13] http://www.guardian.co.uk/world/1999/apr/01/12.

[14] To jedynie liczba działań nagłośnionych przez media o znaczeniu międzynarodowym. Problemy wewnętrznych ataków haktywistów, haktywistyczna walka między państwami oraz ataki nie ujawnione, należy postrzegać w setkach tysięcy. Szczególnie wzmożonym okresem jest ostatnia dekada – co spowodowane jest znacznym rozwojem sieci oraz umasowieniem dostępu do niej.

[15] Przy współpracy ze zwykłymi internautami wykonującymi ich polecenia. Internauci pozyskiwali ze specjalnych stron wiedzę jakie czynności i w jakiej kolejności wykonać, aby wspomóc przypuszczane ataki.

sce w lipcu i sierpniu 2008 roku. W obu przypadkach udało się całkowicie sparaliżować funkcjonowanie sieci www w atakowanych państwach.

Haktywizm po rosyjsku

Rosyjski haktywizm podobnie do demokracji na potrzeby Federacji, został zmodyfikowany i dostosowany do wypełniania woli władzy. O ile bowiem działania haktywistów na całym świecie wymierzone są przeciw rządom, o tyle w Rosji zdają się służyć interesom Federacji. Jako przykład należy przytoczyć tu postawę Federacji Rosyjskiej, która nie tylko nie potępiła akcji crakcerów z 2007 roku, lecz publicznie manifestowała wdzięczność *aktywnym w wirtualnym świecie rosyjskim obywatelom*.

To nie pierwsza tego typu postawa rosyjskich władz. W 2002 roku grupa studentów zaatakowała niezależną witrynę kavkazcenter.com, informującą o nielegalnych działaniach Federacji na terenie Kaukazu Północnego. Od momentu powstania strona ta jest jednym z najczęstszych obiektów zamachów rosyjskich haktywistów. W odpowiedzi rządowej na zarzuty tłumienia wolności słowa poprzez ataki na wyżej wymienioną witrynę – dyrekcja FSB wydała oświadczenie, jakoby ataki były *wyrazem obywatelskiej postawy wobec terrorystów kaukaskich*.

W 2005 roku powstała oficjalna grupa haktywistów rosyjskich *Obywatelski Antyterror*, która za główny cel obrała sobie prowadzenie cyfrowej wojny z *czeczeńskimi terrorystami*. Co istotne, w przeciwieństwie do światowych haktywistów – grupa rosyjska posiada przywódców oraz niezwykle sprawną koordynację działań w sieci. *Obywatelski Antyterror* zajmuje się także sporządzaniem szczegółowych instrukcji *krok po kroku* dla przeciętnych użytkowników, które pozwolą im dokonać ataku na niezależne serwisy informujące o sytuacji na Kaukazie.

Regularnie atakowane są także strony opozycji, a sprawnie funkcjonujące służby antyterrorystyczne nie są w stanie namierzyć sprawców.

Podejmowane przez rosyjskich haktywistów walki z państwami skonfliktowanymi z Federacją oraz mocne wsparcie strony rządowej, przeświadczają międzynarodowych specjalistów o współpracy obu środowisk oraz nieuchronnie zbliżającym się zagrożeniu cybernetycznym ze strony Rosji.

Współczesny haktywizm

Haktywiści, podobnie jak pierwsza użytkowa wersja narzędzia, którym się posługują (Internet) pojawili się w Stanach Zjednoczonych Ameryki Północ-

nej[16]. Choć ta forma cybernetycznego obywatelskiego nieposłuszeństwa znana była tam od wielu lat, a pierwsi z przedstawicieli tego ruchu czynnie działali od końca lat 80. – świat po raz pierwszy usłyszał o nich w pełni dzięki ruchowi ANONYMOUS.

Wywodząca się z serwisu 4chan.org grupa użytkowników o niestałym składzie swój pierwszy haktywistyczny atak przypuściła w imię walki z sektami przeciw kościołowi scientologicznemu w styczniu 2008 roku.

Poprzez setki ataków typu DDoS na witryny sekty oraz związanych z nią organizacji – skutecznie blokowano działalność ugrupowania. Nie mogąc równać się wiedzą oraz sprytem z działaczami wirtualnymi, scientolodzy przenieśli swą batalię z haktywistami do świata rzeczywistego. Wynikiem licznych pozwów w chwili kilkunastu członków Anonymous zostało skazanych na karę pozbawienia wolności za działalność cyberprzestępczą.

Sądowa batalia scjentologów z członkami Anonymous, przyczyniła się do schizmy dotąd jednogłośnej grupy użytkowników 4chan.org. Część osób korzystających z portalu jedynie w celach rozrywkowych nie chciała brać udziału w poważnych akcjach o profilu społeczno-politycznym. Nastąpiło starcie ideologii, które zaowocowało rozłamem userów na obóz 4chan oraz Anonymous. Doprowadziła do tego akcja pierwszej grupy hakerów, którzy chcąc zniszczyć opinię Anonymus (odciągając tym samym od siebie podejrzenia FBI) dokonała w imieniu anonimowych sabotażu portalu dla chorych na epilepsję.

Znacznie poważniejsze następstwa przyniosła batalia rządów światowych z portalem WikiLeaks posiadającym jednocześnie swe wczesne korzenie w ruchu Anonymous.

Kiedy do działań politycznych przyłączyły się serwisy płatnicze Mastercard i PayPal, które odcięły możliwość finansowania WikiLeaks, pozostawiając tym samym możliwości finansowania m.in. stronom propagującym ruchy neonazistowskie i skrajne ruchy socjalistów, zamach na portal obywatelskiego nieposłuszeństwa uznano za międzynarodową próbę zamknięcia ust obywatelom walczącym o triumf prawdy. Wywołało to falę ataków ze strony haktywistów. Zdjęto stronę Federalnego Sądu Apelacyjnego w San Francisco oraz komercyjnych firm np. Sony Playstation. W ramach odwetu za pozwanie przez firmę Sony George Hotza – domorosłego programisty, Anonymous ponad 20 razy w ciągu zaledwie 8 miesięcy włamywał się na serwery firmy kradnąc i rozrzucając w Internecie poufne dane

[16] Istnieją współcześnie spory co do twórcy idei Internetu (wymieniając m.in. Amerykanina Lawrencea Roberta, Amerykanina polskiego pochodzenia Paula Barana, a nawet belgijskiego naukowca Paula Otleta z jego ideą z 1934 roku), jednakże pierwsza użytkowa wersja powstała w USA na zamówienie Pentagonu.

ponad 77 milionów użytkowników. Zawieszenie działania jedynie witryny SONY oszacowano wówczas na straty w wysokości 150 milionów dolarów. W ciągu kilku miesięcy regularnie włamywano się do kont firm bankowych visa, paypal, mastercard. Nazywając Mastercard i PayPal – mafią bankową – dokonywano ataków na ich serwery, notorycznie zdejmowano strony senate.gov, CIA, policji oraz partii politycznych.

Zorganizowany dzięki koordynacji tłum 10 tysięcy rozgniewanych obywateli, udowodnił rządowi Stanów Zjednoczonych, że problemy operacji w Libii, angażowania opinii publicznej w sprawy powstań tunezyjskich, czy słuszności pobytu wojsk w Afganistanie są niczym przy nagłym i skoordynowanym uderzeniu niezadowolonych haktywistów. Ów cios był jednak o wiele bardziej niebezpieczny niż standardowe ataki hackerskie czy terrorystyczne, gdyż przeprowadzony został przez rzeczywistych obywateli własnego kraju, którzy płacą podatki, pracują i nie zamierzają patrzeć jak lobbystyczne grupy rządowe i korporacyjne zamykają usta sprawiedliwym. To działania rządu głuchego na opinię społeczeństwa zdetonowały ładunki emocji obywateli, uświadamiając wszystkim rządom światowym, jak dużą lukę w systemach bezpieczeństwa wewnętrznego posiadały dotychczas. Skoordynowane działania w świecie realnym i cybernetycznym, przyczyniły się do wyprowadzenia tysięcy poufnych dokumentów rządowych i licznych włamań na konta polityków (w tym także prywatne konto e-mail Sary Palin).

Powołany do zwalczania cenzury Anonymous wziął także czynny udział w akcji przeciwko blokowaniu WikiLeaks w Tunezji. Działacze podtrzymywali kontakt rebeliantów z resztą świata. Jako pierwsi wykradli dane dotyczące dyktatora Ben Alego. Przy pomocy Internetu oraz portali społecznościowych Facebook i Tweeter, jednoczyli się w walce, wygrywając ostatecznie z dyktaturą.

Haktywiści wspomagali także w realnej walce Egipcjan. Za pośrednictwem ukrytej poczty przesyłano instrukcje *know – how*, jak obejść zabezpieczenia rządowe. Przesyłki zawierały także informacje dotyczące sposobu konfiguracji dial – up, danych służących do połączeń modemowych oraz częstotliwościach krótkofalówek. Front Anonymous tłumaczył na język arabski instrukcje zachowania się w przypadku ataku gazem, metody leczenia oraz zasady niesienia pierwszej pomocy dla ofiar bezpośredniego ataku. Jednocześnie realizowano dobrze znane haktywistom obciążanie serwerów oraz zdejmowanie internetowych stron rządowych. Mubarak zrezygnował z pełnienia urzędu. Egipcjanie wielokrotnie dziękowali publicznie Anonymous.

Wówczas po raz pierwszy haktywizm przeraził światowy establishment. Rządy całego świata przyznawały słabość własnych zabezpieczeń oraz potrzebę wypracowania lepszych strategii bezpieczeństwa cybernetycznego. Jednocześnie obawy

wzbudziła łatwość, z jaką haktywizm przeniósł się do świata realnego – a co gorsze łatwość, z jaką wpłynął na rozwój strajków w Tunezji i Egipcie.

Haktywizm po polsku

Kontakty Rzeczpospolitej z haktywizmem po raz pierwszy publicznie odnotowano w roku masowych cybernetycznych międzynarodowych akcji aktywistycznych – 1998.

Dwa dotąd odrębne światy w kulturze naszego kraju – realny i jakże odległy wówczas – cybernetyczny, zetknęły się i mimo dużych oporów – rozpoczęły współpracę.

Pierwsza akcja haktywistyczna, transmitowana na żywo 20 czerwca 1997 roku na antenie programu Piotra Najsztuba i Jacka Żakowskiego TOK SZOK, dotyczyła włamania na serwery Ministerstwa Gospodarki i miała charakter pokojowy.

Wówczas to młody haker, który wykrył poważne luki w zabezpieczeniach, na oczach rządowych informatyków odpowiedzialnych za zabezpieczenia, dokonał włamania na serwery przeglądając na wizji poufne informacje. O ile pytanie, czy atak ów posiadał znamiona tzw. klasycznego haktywizmu pozostaje kwestią dyskusyjną[17], o tyle cel oraz sposób działania hackera, bezsprzecznie można określić wartościami haktywistów. Dwóch kolejnych następców włamało się na strony Urzędu Rady Ministrów oraz Centrum Astronomicznego im. M. Kopernika, gdzie uszkodzili systemy operacyjne pokazując, jak banalne zabezpieczenia posiadają polskie placówki rządowe i edukacyjne.

Także wielokrotne działania hackerskiej grupy *Gumisiów* – wymierzone przeciw monopolowi i podwyżkom cen usługi internetowej TP S.A.[18] – Neostrady, polegające na włamywaniu się na stronę firmy oraz podmienianiu jej treści, nosiły znamiona hatywizmu[19].

Technikę „emailowej bomby" zastosowano w ramach protestu na skrzynce internetowej wydawnictwa, które zgodziło się na publikację książki Jana Tomasza Grossa „Strach".

---

[17] Strona rządowa zarzucała wówczas dziennikarzom prowokację przeprowadzoną jedynie w celu zwiększenia oglądalności programu.

[18] http://www.wprost.pl/ar/5235/Wirtualny-wlamywacz/?pg=2#an_619447072.

[19] Dokonując ataków na treści stron TP.SA – *Gumisie* ustawiali ironicznie zmodyfikowane hasło Nokii („Nokia – Connecting People" – Nokia Łączy Ludzi) na „TP S.A. Disconnecting people" (TP S.A. – Rozłącza Ludzi)

W 1999 roku, tj. okresie *raczkowania* polskiego Internetu, odnotowano około 100 prób poważnych włamań do sieci komputerowych. *Oznacza to, że w Polsce pojawiła się generacja hakerów o wiedzy i umiejętnościach na poziomie światowym* – ocenił wówczas Mirosław Maj, pracownik Zespołu Reagującego na Zdarzenia Naruszenia Bezpieczeństwa Sieci NASK.

Największą aktywność haktywistów na polskiej scenie politycznej mogliśmy zaobserwować w styczniu 2012 roku, kiedy to rząd RP bez porozumienia z internautami oraz opinią publiczną postanowił ratyfikować międzynarodowe porozumienie ACTA.

W całym kraju odbyły się protesty przeciwko podpisaniu umowy bez wiedzy i zgody obywateli. Pikieta w Kielcach zakończyła się blokadą skrzyżowania w centrum miasta i uszkodzeniem samochodów. Jeden policjant trafił do szpitala. Zatrzymano 24 osoby. Niszczono znaki drogowe, dewastowano ulice, atakowano Policję. Protestowano w Poznaniu, Gdańsku, Lublinie, Warszawie, Wrocławiu, Krakowie, Łodzi, Bydgoszczy, Toruniu, Szczecinie, Katowicach, Białymstoku, Gdyni, Częstochowie, Sopocie, Radomiu, Kielcach, Rzeszowie. W akcji haktywistów zawieszono strony Sejmu, Ministerstwa Kultury i Dziedzictwa Narodowego, Kancelarii Premiera, Stowarzyszenia Autorów ZAiKS, Kancelarii Prezydenta oraz Policji.

Wystąpienia publiczne rzecznika rządu oraz dyrekcji biur prasowych, bagatelizujące ich działania, które określano *wyłączeniem stron ze względu na awarię*[20] jedynie rozjuszyły haktywistów. Dużą pomysłowością wykazał się Paweł Graś, który stwierdził że *trudno mówić o ataku hackerów, a jedynie o dużym zainteresowaniu treściami na stronach Premiera i Sejmu. Jest to oczywiste — wiele osób w weekend wchodzi na strony rządowe, aby nadrobić zaległości*[21].

Do zablokowania najważniejszych stron przyznali się haktywiści Anonymous: „sejm.gov.pl – Tango down" (slogan oznaczający zdjęcie wroga – przyp. autora). Przed kolejnym wyłączeniem pojawił się na stronie napis: „Nie ma rzeczy niemożliwych. Pozdro panowie!". Tego samego dnia na koncie Twittera anonimowi podali do wiadomości, że zbierają kompromitujące informacje o rzeczniku rządu Pawle Grasiu i niebawem ujawnią je w Internecie.

O krok dalej posunęła się polska grupa hakerów *Polish Undergound*, która włamała się na stronę internetową Prezesa Rady Ministrów, dokonała podmiany treści umieszczając filmik z popularną celebrytką internetu naśladującą gen. Jaruzelskie-

[20] http://wiadomosci.wp.pl/kat,1329,title,Polskie-strony-rzadowe-przestaly-dzialac Protestprzeciwko-ACTA,wid,14187932,wiadomosc.html?ticaid=1f948&_ticrsn=3.

[21] http://www.dobreprogramy.pl/Eskalacja-protestow-przeciwko-ACTA-podmieniono -strone-glowna-Premiera,Aktualnosc,29928.html.

go[22]. Incydent ten w opinii pozostałych haktywistów określony został mianem przekroczeniem granicy. Dotychczasowe działania mające na celu zaspamowanie i zablokowanie serwerów nosiły jedynie znamiona protestu. Część środowisk haktywistycznych nie chciała być kojarzona z przekroczeniem granicy prawa. Wizerunek cybernetycznych aktywistów zniweczyła także deklaracja *Polish Underground,* która w sposób dobitny wskazywała jak bardzo heterogeniczne jest środowisko haktywistów *Nie należymy do Anonymous. Anonimowi nie są hakerami, to dzieci, które chciały się pobawić w hakerów*…

Z kolei Anonymous Polska twierdził, że posiada dokumenty, które zostaną ujawnione w przypadku podpisania przez władze RP ACTA. Poświadczeniem realności tych gróźb była potwierdzona w mediach informacja o włamaniu do komputera wiceministra Ministerstwa Administracji i Cyfryzacji. Co istotne, nad regulacjami w sprawie ACTA strona rządowa pracowała od 2006 roku, zaś pierwszą wersję porozumienia mogliśmy poznać właśnie dzięki grupie wyodrębnionej z Anonymous – Wikileaks.

Wynikiem przeniesienia strajków w obie sfery: do świata rzeczywistego i wirtualnego, rząd RP odstąpił od zamiaru podpisania umowy, zaś polscy haktywiści pokazali jak we współczesnym świecie cyfrowym i realnym należy traktować informacje. Nie wybiórczo, nie pobieżnie, nie potajemnie, ale jawnie i rzetelnie.

Zagrożenie bezpieczeństwa

Haktywizm jest zupełnie nowym zjawiskiem, które we współczesnym świecie stanowią rzadkość. Jako takie wymaga zatem uwagi, analizy oraz pogłębionej refleksji.

Mimo, iż mianem haktywistów nazywamy współcześnie specjalistów wykorzystujących (często nielegalnie) narzędzia rozwiniętej technologii oraz umiejętności hackerskie w szeroko pojętym interesie społecznym – ich pobudki oraz motywacje nie zawsze należały do altruistycznych.

Warto wspomnieć tu chociażby o akcjach użytkowników 4chan.org, którzy dla zabawy wkleili stroboskopowe animacje na forum dla chorych na epilepsję, co owocowało tysiącami ataków u przeglądających je chorych. Hakerzy ci narażali życie niewinnych osób jedynie dla zabawy.

Współczesnym haktywistom przyświecają zatem różne cele. Heterogeniczność tego środowiska można z powodzeniem porównać do ruchu alterglobalistów. Zło-

[22] Stanowiło to odwołanie do wprowadzenia przez Jaruzelskiego stanu wojennego oraz masowych pacyfikacji społeczeństwa.

żone z licznych mikro grup o całkowicie odmiennych ideologiach, poglądach politycznych, religijnych i społecznych – mogą w równym stopniu służyć społeczeństwu, jak i doprowadzić do jego zniszczenia. Działacze ci, ze względu na swoją heterogeniczność środowiskową oraz nieprzewidywalne możliwości mogą wbrew szczytnym celom nieść zniszczenie i śmierć. Środowisko haktywistów skupionych wokół różnych idei oraz różnych portali, rządzi się ustalanymi ad hoc prawami, nie zawsze przemyślanymi i spójnymi wewnętrznie. Może o tym świadczyć chociażby apel hakerów nazywanych w środowisku *old time hactivists*, skierowany do swoich współczesnych następców: „Przekroczyliście granice!"[23].

Ich działalność stanowi także problem dla wewnętrznego bezpieczeństwa państwa. Docierający w jednej chwili do milionów ludzi aktywiści, mają moc przekazywania światu wiadomości odbieranych jako pewne i sprawdzone. Nie trudno sobie wyobrazić zatem możliwą manipulację społeczeństwem. Działacze dokonujący kilku mniejszych społecznych akcji aktywistycznych, zyskując zaufanie, mogą wykorzystać ów kredyt do zorganizowania akcji służącej jedynie ich prywatnym, partykularnym interesom.

Obsmarujmy kogoś na jakiejś stronie! – Gregg Housh – hatywista kojarzony z portalem 4chan.org.

Uzasadnione pytanie budzi także obawa o prawo do działania i jego granice w określonych przypadkach. Przykładem może być tu osoba Halla Turnera właściciela stron oraz podcastów wiązanych z ruchami rasistowskimi. Członkowie 4chan.org uznając, iż posiadają *wyższość moralną*[24], zawiesili działalność jego stron. W swoich działaniach posunęli się jednak o krok dalej. Ofierze zamawiano zakupy do domu, pizze, usługi prostytutek, palety z materiałami przemysłowymi. W ciągu kilku dni zniszczono go finansowo – a poprzez ujawnienie jego powiązań z FBI przy inwigilacji środowiska neonazistowskiego – narażono także jego życie.

Bardzo dobrze zrobiło nam to na ego. Ludzie zobaczyli że są nas tysiące. Byliśmy w tym momencie władcami świata.[25]

Kolejne niebezpieczeństwo budzi łatwość z jaką odpowiednie grupy/osoby mogą przeniknąć do anonimowego świata haktywistów, a przy pomocy zabiegów socjotechnicznych i odpowiedniej perswazji, sprowokować internetowych aktywistów do podjęcia działań zgodnych z sugestiami proponującego.

---

[23] http://news.cnet.com/8301-27080_3-57406793-245/old-time-hacktivists-anonymous-youve-crossed-the-line/.

[24] Wypowiedź użytkownika 4chan.org, współorganizatora akcji.

[25] Wypowiedź członka Anonymous po przeniesieniu wirtualnych strajków antyscjentologiczych do realnego świata. Zarejestrowana w filmie *We are Legion*, 2012, Canal+ Polska.

Niebezpieczna z punktu widzenia bezpieczeństwa państwa jest także interpretacja działalności haktywistów. Czy protestujący przeciw złej polityce rządu haker aktywista prowokujący społeczeństwo do buntu, wystąpień i strajków, winien być postrzegany jako lider współczesnego, cyfrowego odpowiednika Solidarności? A może winien zostać pojmany przez agencję zajmującą się bezpieczeństwem wewnętrznym za próby destabilizacji państwa?

Czy włamanie na stronę rządową z pobudek haktywistycznych winno być traktowane na równi z zamachem na niezawisłą władzę, atakiem cybernetycznym, a może cyberterroryzmem? Czy osoba taka winna być skazana? Czy jest to przejaw obywatelskiego nieposłuszeństwa, akt przestępczy, a może czyn wandala? Czy odmianą haktywizmu można nazwać już obciążenie linii programu o zabarwieniu politycznym transmitowanego na żywo?[26] Czy w imię wolności słowa hackownanie stron krytyków ruchu haktywistycznego[27] pozostaje dalej walką w słusznej sprawie?

Trudno także rozróżnić, czy dokonywane ataki są działaniami haktywistycznymi, stricte hackerskimi/crackerskimi, czy już cyberprzestępczymi. Czy dokonujący za zgodą koalicji włamań w czasie operacji Pustynna Burza na irackie serwery, działacze byli haktywistami – wojownikami o wolność Kuwejtu, działali dla własnego interesu[28], czy też na zlecenie rządów państw koalicyjnych?

Jedno jest pewne. Ambicje i poziom wiedzy haktywistów stale rosną, zaś wiedza rządów oraz działania podejmowane względem ruchu zdają się tkwić w martwym punkcie – co sugestywnie wskazują bieżące wydarzenia związane z tego rodzaju atakami. Haktywiści po pierwszym udanym uderzeniu, zrozumieli jaką siłą dysponują. Zwykłe, dotąd szare jednostki zrozumiały, że mogą bezkarnie wpływać na geopolitykę świata, nie wychodząc z domu, nie odczuwając żadnej presji, nie ponosząc żadnej odpowiedzialności moralnej.

Poza walką z rządami poprzez blokowanie stron, cybernetyczni aktywiści zaangażowali się w sposób czynny również w realnych konfliktach. Pomagali Libij-

---

[26] Mowa tu o polskim programie *Szkło kontaktowe*, który ponad 4 razy aktywni działacze cybernetyczni w ramach walki z poglądami prowadzącego – regularnie blokowali. Obciążano wówczas linię telefoniczną, będącą jednocześnie ważnym elementem dyskusji politycznych.

[27] W Stanach Zjednoczonych Ameryki Północnej Anonymous wielokrotnie hackował, bądź poprzez zmianę treści witryn, przyczyniał się do narażenia utraty dobrego imienia (treści pedofilskie, nekrofilskie, homoseksualne) dziennikarzy, którzy otwarcie krytykowali kierunek, w którym zmierza ruch.

[28] Mowa tu o bezkarnych działaniach przyczyniających się do poszerzenia własnej wiedzy i doświadczenia, których w warunkach pokoju działacze Ci nie mieliby prawa wykonywać pod groźbą pozbawienia wolności.

czykom, Tunezyjczykom i Egipcjanom w walce z tyranią, wspierali Australijczyków w walce z planami wprowadzenia na Antypodach cenzury Internetu[29]. W Polsce kilka niezależnych grup aktywistycznych na czele z Anonymous Polska, przy pomocy portali społecznościowych, zorganizowało strajki przeciw ratyfikacji ACTA. W ostatnich dniach haktywiści opowiedzieli się po stronie Strefy Gazy w konflikcie palestyńsko-izraelskim[30].

Zakończenie

Bez wątpienia haktywizmu nie można określać jedynie mianem zagrożenia. Podejmowane przez ruch działania posiadają najczęściej szczytne cele, a koszty takich operacji pokrywają sami aktywiści. W wielu przypadkach akcje te pozostają jedyną deską ratunku dla społeczności. Niestety, zagrożenie stwarza brak wewnętrznych struktur oraz wzajemnej kontroli[31]. W ruchu haktywistycznym panują jednocześnie anarchia i demokracja.

Reprezentując chaos wolności, dzięki swym umiejętnościom posiadają realny wpływ nie tylko na geopolitykę świata, lecz również politykę wewnętrzną własnego państwa. To zjawisko piękne i poruszające, ale niestety także przerażające. Rządy państw bagatelizujące znaczenie Internetu oraz jego działaczy – zasługują na dymisję, co jasno artykułują nie tylko cyfrowi aktywiści, lecz również specjaliści od bezpieczeństwa[32]. Haktywiści mogą być kim zechcą, gdzie zechcą i kiedy zechcą. Namierzenie ich jest o wiele trudniejsze niż zlokalizowanie siedziby Talibów, czy grupy przemytniczej. W jednej sekundzie mogą być w Japonii, aby w kolejnej znajdować się w Europie Zachodniej. Ich podróże ogranicza jedynie prędkość łącza internetowego a możliwości rosną proporcjonalnie do ignorancji władz państwa.

Niepokojący jest kierunek ewolucji haktywizmu oraz sposób wykorzystywania pozyskanych informacji. Od obywatelskiego nieposłuszeństwa, poprzez sprzeciw internetowy, protest w sposób niewyrządzający nikomu krzywdy, aż po angażowanie się w konflikty zbrojne oraz przenoszenie działań ze świata cyfrowego do

---

[29] http://technologie.gazeta.pl/internet/1,104530,7612128,Haktywisci___hakerzy_w_sluzbie_spoleczenstwa.html.

[30] Ogłoszenie Anonymous z dn. 15.11.2012 r. umieszczone na tysiącach portali informacyjnych m.in. Facebook, Twitterze, Youtube etc.

[31] Intencje autora doskonale odzwierciedla tu jedna z planowanych akcji Anonymous konsultowana na portalu 4chan.org.

[32] Taką opinię wyraził m.in. amerykański filozof i strateg bezpieczeństwa – Joshua Corman.

rzeczywistego. Szczególną uwagę należy zwrócić na ostatnią wypowiedź Anonymous dotyczącą niezwykle trudnego i delikatnego konfliktu palestyńsko-izraelskiego: „Obywatele świata. Jesteśmy Anonymous. Zbyt długo wraz z resztą świata obserwowaliśmy barbarzyńskie, brutalne i niemożliwe do opisania traktowanie Palestyńczyków na tak zwanym terytorium okupowanym, największym więzieniu na świecie. […] Jednak w momencie, gdy rząd Izraela publicznie zagroził zerwaniem Internetu oraz wszelkich usług telekomunikacyjnych w Strefie Gazy, przekroczył granicę wytyczoną na piasku. Jak były dyktator Egiptu – Mubarak odczuł na własnej skórze – jesteśmy Anonymous i NIKT na naszej warcie nie ma prawa odłączania kogokolwiek od Internetu. Do ludu Gazy i terytoriów okupowanych – wiedzcie, że Anonymous staje obok was do walki”[33]. Zauważalny ton oraz charakter polityczny wypowiedzi stanowić może potwierdzenie zaprezentowanych powyżej obaw autora.

Znany z ataku na łotewski urząd skarbowy haktywista NEO, dzięki luce w systemie elektronicznych deklaracji podatkowych, pozyskał ponad 120gb danych dotyczących zarobków najbogatszych Łotyszy[34], a następnie doprowadził do ich wycieku. O ile idea była szczytna, o tyle nieprzemyślane działania grupy *Czwartej Ludowej Armii Przebudzenia* mogły doprowadzić do daleko posuniętej destabilizacji państwa.

Wziąwszy pod uwagę ówczesną sytuację ekonomiczną i gospodarczą kraju, gdzie PKB spadło o ok. 18%, a bezrobocie osiągnęło poziom 22,8%, informacja ta mogła doprowadzić do eskalacji konfliktu między społeczeństwem a władzą, który mógł przerodzić się nawet w wojnę domową[35].

„Haktywiści są łobuzami aktywizmu. Jest w nich coś nieogładzonego i właśnie to sprawia, że budzą tak różne reakcje”[36].

---

[33] Wypowiedź z dn. 15.11.2012 r., http://www.youtube.com/watch?v=O6t9Kr2wWzE (dostęp: 16.11.2012 r.).

[34] http://wyborcza.biz/biznes/1,101562,7603194,Lotewski_Robin_Hood_wytyka_bogaczom_zarobki.html.

[35] To kolejny przykład niejasnych motywów działań haktywistów. Nękana problemami ekonomicznymi Łotwa, starająca się o otrzymanie ponad 7,5 mld euro pomocy międzynarodowej, zobowiązała się do przeprowadzenia drastycznych cięć budżetowych. Obniżki pensji dosięgnęły niemal wszystkich grup społecznych. Jednocześnie haktywiści dokonywali na portalu informacyjnym Twitter regularnego szczucia określonych grup społecznych na siebie. Jedna z odezw brzmiała: Wzywam związek zawodowy policjantów do przeanalizowania danych, zastanowienia się czy reforma płac jest sprawiedliwa i do dalszej walki z przestępczością…

[36] Opinia G. Colleman z Uniwersytetu McGill USA, wyrażona w filmie dokumentalnym pt. „Jesteśmy Legionem – historia haktywizmu” 2012, Canal+ Polska.