Marlena Piotrowska

Haktywizm - społeczna korzyść czy zagrożenie?

Studia Humanistyczne AGH 16/2, 25-40

2017

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

MUZEUM HISTORII POLSKI

http://dx.doi.org/10.7494/human.2017.16.2.25

Marlena Piotrowska*

Uniwersytet Wrocławski

HAKTYWIZM – SPOŁECZNA KORZYŚĆ CZY ZAGROŻENIE?

Artykuł koncentruje się na tematyce haktywizmu, który od lat 80. XX wieku łączy świat technologii ze światem polityki. Haktywizm jest bowiem połączeniem aktywizmu społeczno-politycznego z hakerstwem. Celem badania jest ocena haktywizmu pod kątem szans i zagrożeń, jakie niesie ze sobą to zjawisko. Problem badawczy niniejszego artykułu sprowadza się do pytania, czy haktywizm jest społeczną korzyścią, czy zagrożeniem? Główną tezą jest stwierdzenie, że haktywizm nie stanowi poważnego zagrożenia dla ogółu społeczeństwa i struktur państwa. W artykule został przedstawiony przegląd najważniejszych definicji haktywizmu oraz metody działań haktywistów wraz z przykładami z XXI wieku. Podjęto się również próby oceny tego zjawiska pod kątem szans i zagrożeń, jakie niesie dla obywateli i instytucji państwowych, a także zaprezentowano prognozowany kierunek rozwoju haktywizmu.

Słowa kluczowe: haktywizm, elektroniczne nieposłuszeństwo obywatelskie

WSTĘP

Wiele sfer działalności człowieka uległo znacznym przeobrażeniom w XXI wieku. Postęp technologiczny, z którym mamy współcześnie do czynienia, a w szczególności bardzo duża popularność mediów społecznościowych, usieciowienie, wpłynęły na zmianę życia codziennego człowieka, w tym również na przeobrażenie mobilizacji politycznej. Jedną z wielu form aktywności człowieka w Internecie jest haktywizm łączący sferę technologii i płaszczyznę interesów społeczno-politycznych. Sam termin „haktywizm" jest nieostry i może być mylnie utożsamiany z innymi zjawiskami, co zostanie omówione w dalszej części artykułu.

Celem artykułu jest ocena haktywizmu pod kątem szans i zagrożeń, jakie niesie ze sobą to zjawisko. Problem badawczy sprowadza się do pytania, czy haktywizm jest społeczną korzyścią, czy zagrożeniem? Główną tezą jest stwierdzenie, że haktywizm nie stanowi poważnego zagrożenia dla ogółu społeczeństwa i struktur państwa. Mimo to jest bardzo prawdopodobne, że w ogólnej kalkulacji przynosi więcej szkód niż korzyści dla społeczeństwa. Należy przypuszczać, że aktywistom nie zależy na dokonaniu zniszczeń. Na początku zostanie przedstawiony przegląd najważniejszych definicji haktywizmu, następnie techniki haktywistów

* Adres do korespondencji: Marlena Piotrowska, Instytut Politologii, Wydział Nauk Społecznych Uniwersytetu Wrocławskiego, ul. Koszarowa 3, 51-149 Wrocław; e-mail: marlena.piotrowska@uwr.edu.pl.

wraz z przykładami ich działań w XXI wieku. Na końcu zostanie podjęta próba oceny tego zjawiska pod kątem szans i zagrożeń, jakie niesie dla obywateli i instytucji państwowych.

HAKTYWIZM – KWESTIE DEFINICYJNE

Wśród badaczy haktywizmu nie istnieją szczególne spory definicyjne. Problem stanowi na ogół umiejscowienie tego zjawiska: niektórzy traktują je jako przejaw internetowej mobilizacji, inni natomiast sytuują haktywizm wśród przykładów działań przestępczych w przestrzeni wirtualnej. Tim Jordan i Paul Taylor utożsamiają haktywizm z mieszanką oddolnego protestu politycznego i hakerstwa komputerowego (Jordan i Taylor 2004: 1). Natomiast Alexandra Samuel w swojej pracy doktorskiej definiuje haktywizm „jako pokojowe użycie nielegalnych lub niejednoznacznie legalnych cyfrowych narzędzi w dążeniu do osiągnięcia celów politycznych" (Samuel 2004: 2). Amerykańska badaczka Dorothy Denning zauważa z kolei, że: „haktywizm obejmuje działania wykorzystujące techniki hakerskie przeciwko witrynie internetowej z zamiarem zakłócenia jej normalnego funkcjonowania, a nie spowodowania poważnych szkód" (Denning 2001: 241). Warto uzupełnić to wyjaśnienie o spostrzeżenia Jordana i Taylora, którzy podkreślają to, co znamienne dla haktywizmu, czyli bezpośredniość działań podejmowanych w Internecie w celu wywołania natychmiastowych zmian w sferze politycznej (Jordan i Taylor 2004: 67–68). Mirosław Lakomy zauważa, że „haktywiści wykorzystują cyberataki do promocji określonych postaw, wartości lub idei politycznych lub aby zwrócić uwagę opinii publicznej na określone problemy" (Lakomy 2015: 145). Ponadto autor uznaje haktywizm za jedną z metod sieciowej demokracji obywatelskiej (*netizen democracy*[1]), która wiąże się z wykorzystaniem nowych mediów między innymi w celu wyrażenia sprzeciwu wobec prowadzonej polityki, co można utożsamiać ze współczesną partycypacją w procesach demokratycznych (Lakomy 2013: 269). Do celów niniejszego artykułu najbardziej przydatna jest definicja haktywizmu w ujęciu Andrzeja Chodubskiego, według której haktywizm to „ruch kulturowo-cywilizacyjny polegający na łączeniu aktywności politycznej z osiągnięciami technologicznymi, w celu manifestowania sprzeciwu wobec działań w przestrzeni szeroko rozumianej polityki" (Chodubski 2014: 125).

Wielu badaczy utożsamia haktywizm z aktami wirtualnego nieposłuszeństwa obywatelskiego (*Electronic Civil Disobedience* – ECD)[2]. Jak twierdzą Marta du Vall i Marta Majorek, w „XXI wieku haktywizm jest jedną z form walki przeciwko określonemu porządkowi politycznemu, polityce wewnętrznej lub zagranicznej państwa, panującym w danym państwie stosunkom ekonomicznym lub pewnym instytucjom prawnym. Jest więc niczym innym jak przejawem obywatelskiego nieposłuszeństwa" (du Vall i Majorek 2013: 30). Wirtualne nieposłuszeństwo obywatelskie jest uznawane przez T. Jordana jako jeden z typów haktywizmu.

[1] *Netizen* to złożenie słów *Net* (sieć) i *Citizen* (obywatel). Autorem terminu jest Michael Hauben. Szerzej: M. Hauben, *The Net and Netizens: The Impact the Net has on People's Lives*, http://www.columbia.edu/~rh120/ch106.x01 [05.04.2016].

[2] Twórcą terminu ECD jest członek grupy artystów aktywistów zwanej Critical Art Ensemble (CAE). Szerzej na ten temat: Critical Art Ensemble, *Electronic Civil Disobedience & Other Unpopular Ideas*, http://www.critical-art.net/books/ecd/ [04.04.2016].

Drugim typem, według autora, jest sprzeciw wobec ograniczania wolności dostępu do informacji w sieci i walka na różne sposoby w obronie tych wartości. Według Jordana zajmują się tym haktywiści informacyjni (Jordan 2011: 90–93). Koncentrując się na obszarach aktywności haktywistów, warto zaznaczyć, że bardzo często ich działalność dotyczy nie tylko sfery politycznej, ale też ekonomicznej.

Wśród wielu zjawisk powiązanych z haktywizmem i bardzo często z nim utożsamianych są hakerstwo i cyberterroryzm. Warto przy tym podkreślić, że często te same zdarzenia są różnie interpretowane ze względu na nieostre granice pomiędzy zjawiskami i brak jednomyślności badaczy co do definicji danych terminów. Coś, co jedni traktują jako cyberterroryzm, inni uznają za jeden z typów haktywizmu – elektroniczne nieposłuszeństwo obywatelskie. Różnice między zjawiskami zacierają się szczególnie w publicystyce i w języku potocznym[3]. W prasie podkreśla się kontrasty między hakerami a haktywistami, nazywając tych pierwszych przestępcami, a drugich ludźmi działającymi w interesie społecznym. Bardzo często różnice między poszczególnymi grupami wyznaczają motywacje i intencje członków grupy. Kluczem do zrozumienia haktywizmu jest poznanie hakerstwa, ponieważ to z niego wywodzi się to zjawisko. W latach 80. XX wieku za hakera uważano osobę, która wykorzystuje własną wiedzę do łamania zabezpieczeń w systemach komputerowych w celu zdobycia dostępu do danych w nich zawartych. Jej zamiarem nie było dokonanie zniszczeń, a jedynie chęć sprawdzenia własnych umiejętności (Terlikowski 2009: 88–89). Współcześnie jednak działania hakerów interpretuje się na podstawie mniej idealistycznych zamiarów. Jak zauważa Marcin Terlikowski, tak zdefiniowani hakerzy nie stanowią dużego zagrożenia dla stanu bezpieczeństwa teleinformatycznego państwa. Większe zagrożenie mogą powodować osoby, które wykorzystują podobne do hakerów metody, jednak określa się je mianem krakerów (*cracker*) lub pseudohakerów. Od hakerów odróżniają ich zamiary – krakerom zależy na wyrządzeniu szkód w systemach informatycznych. Terlikowski sugeruje jednak, by nazywać ich pseudohakerami, mając jednocześnie na uwadze, że grupa ta jest niejednolita – zaliczają się do niej zarówno amatorzy, jak i wysocy specjaliści w dziedzinie informatyki (Terlikowski 2009: 99–101).

W kontekście powyższych rozważań kolejnym ważnym terminem, który należy wyjaśnić, jest cyberterroryzm. Według M. Terlikowskiego, jest to „działalność terrorystyczna, w której programy i urządzenia elektroniczne oraz systemy teleinformatyczne spełniają funkcję specyficznego rodzaju narzędzia – broni w rękach terrorystów" (Terlikowski 2009: 111). Jak się okazuje, ataki cyberterrorystyczne mogą mieć bardzo poważne skutki nie tylko dla funkcjonowania systemów teleinformatycznych, lecz również dla codziennego życia człowieka, ponieważ przynoszą duże straty fizyczne i wiele ofiar śmiertelnych. Należy jednak przypuszczać, że często rządzący nie mają dostatecznej wiedzy rozróżniającej wszystkie zjawiska. W związku z tym każdą działalność człowieka w przestrzeni cybernetycznej, która zagraża bezpieczeństwu, nazywają cyberterroryzmem. Stosowanie tego typu uproszczeń może również świadczyć o celowym demonizowaniu sytuacji.

[3] Przykładem może być artykuł dotyczący przestępstw w sieci, w którym autor uważa, że za atakiem robaka WANK stali krakerzy, a nie haktywiści. Por.: *Tajemnicze przestępstwa w sieci*, http://technowinki.onet.pl/militaria/tajemnicze-przestepstwa-w-sieci/4kl7s [05.04.2016].

Uzupełniając powyższy katalog zjawisk, warto również zwrócić uwagę na slaktywizm (*slacktivism*). Jest to termin będący mieszanką angielskich słów *slacker* (próżniak, leń) oraz *acktivism* (aktywizm). Działania slaktywistów ograniczają się do kliknięcia *Lubię to!* na Facebooku, przyłączeniu się do wydarzenia, obserwowaniu i popieraniu pomysłów w mediach społecznościowych oraz podejmowaniu podobnych działań. Wszelka działalność slaktywistów ogranicza się wyłącznie do klikania myszką w przestrzeni wirtualnej. Nie przekłada się to natomiast na aktywność danej osoby w realnym życiu[4]. Podsumowując dotychczasowe rozważania definicyjne, należy zaznaczyć, że powyższe przykłady zjawisk związanych z haktywizmem nie wyczerpują listy działań człowieka w przestrzeni wirtualnej. Jest to spowodowane złożonością życia społeczno-politycznego.

POWSTANIE HAKTYWIZMU

Korzenie ruchu haktywistycznego sięgają lat 80. XX wieku i są ściśle związane z rozwojem *hakingu*. Tim Jordan, nawiązując do koncepcji genealogii Michaela Foucaulta, proponuje wyodrębnienie czterech faz historii *hakingu*. Pierwszy okres związany był z powstaniem uwarunkowań sprzyjających funkcjonowaniu społeczeństwa w cyberprzestrzeni. Drugi etap, zdaniem Jordana, wiązał się z rozwojem crackingu, co autor uwydatnia, nazywając tę fazę „złotą erą" (*the golden age*) *hakingu* i *crackingu.* Haktywizm wraz z rozwojem cyberprzestępczości, nowym znaczeniem wolnego oprogramowania (*free software*) i pojawieniem się otwartego oprogramowania (*open source*) wpisał się w trzecią fazę. Natomiast czwarty etap w historii tego zjawiska wiąże się między innymi z finansowaniem hakerów przez państwa (Jordan 2016: 1–17)[5]. Jest rzeczą interesującą, że *haking* początkowo miał pozytywne konotacje. Kojarzony był bowiem z posługiwaniem się wysokimi umiejętnościami informatycznymi do złamania zabezpieczeń w systemach komputerowych w celu wykorzystania danych w nich zawartych. Początkowo motywacje hakerów interpretowano pozytywnie – traktowano ich jako osoby, które próbują sprawdzić swoje umiejętności, a także jako specjalistów przyczyniających się w ten sposób do postępu w tej dziedzinie. W kolejnych latach hakerzy podzielili się na wiele nurtów (Lakomy 2015: 138–140). Haktywizm zrodził się z pierwotnej, etycznej formy *hakingu*. W literaturze za początek działań haktywistów uznaje się rok 1989, kiedy dzięki robakowi o nazwie WANK (*Worms Against Nuclear Killers* – Robaki przeciwko nuklearnym zabójcom) został zaatakowany system informatyczny NASA i Amerykańskiego Departamentu Energii (Lakomy 2015: 142–143). Koncentrując się na celu ataku, należy podkreślić, że haktywiści nie mieli zamiaru dokonać zniszczeń, a jedynie zaakcentować problem. W latach 90. XX wieku rozwój technologii przeplatał się ze zwiększaniem świadomości i odrębności haktywistów. Jednakże sam termin haktywizm powstał dopiero w 1996 roku. Jego autorem jest członek grupy Cult of The Dead Cow (Lakomy 2015: 143). Jak zauważa M. Lakomy:

[4] O. Święcicka, *Generacja leni – slaktywiści. Czy można zbawić świat, klikając myszką?*, http://natemat.pl/34501-,generacja-leni-slaktywisci-czy-mozna-zbawic-swiat-klikajac-myszka [06.04.2016].

[5] W kontekście rozwoju haktywizmu warto przyjrzeć się szerzej koncepcji genealogii *hakingu* prezentowanej przez Tima Jordana (Jordan 2016: 1–17).

„w tym pierwotnym ujęciu za haktywistę uznawano osobę stosującą techniki hakerskie do promocji określonych idei lub postaw politycznych" (Lakomy 2015: 143). W połowie 2001 roku grupa Cult of The Dead Cow (cDc) i jej odłam, Hactivisimo, opublikowali *The Hactivisimo Declaration*, nawiązującą między innymi do Powszechnej Deklaracji Praw Człowieka oraz Międzynarodowego Paktu Praw Obywatelskich i Politycznych, w której zawarli sprzeciw wobec pogwałcenia przez państwa i korporacje wolności informacji w Internecie i sformułowali swoisty kodeks postępowania haktywistów[6].

Duże znaczenie dla rozwoju haktywizmu miało powstanie w 2003 roku serwisu 4chan.org. To właśnie tam, dzięki formule działania serwisu (anonimowi użytkownicy mieli możliwość publikowania dowolnych treści, często były to kontrowersyjne materiały), mogli „gromadzić się" hakerzy o odpowiednich poglądach politycznych. Początkowo akcje były traktowane jako forma rozrywki i seria wygłupów, następnie ewoluowały w kierunku systematycznej „wojny". To właśnie dzięki temu portalowi zrodziła się znana grupa haktywistów – Anonymous[7]. Jednym z najbardziej medialnych działań grupy był *Project Chanology*, kiedy Anonimowi wystąpili przeciwko Kościołowi scjentologicznemu, który miał zamiar walczyć w sądzie z osobami krytykującymi tę sektę. Zdaniem haktywistów w ten sposób Kościół scjentologiczny próbował ograniczać wolność wypowiedzi. Wtedy też Anonimowi opublikowali w Internecie pierwszy film o sobie samych – ich znakiem rozpoznawczym stała się maska Guya Fawkesa[8] (Macała 2014: 172–173). Maski na twarzach miały podkreślać symboliczną i praktyczną anonimowość członków grupy – stały się wyróżnikiem, a zarazem uniemożliwiały odkrycie tożsamości Anonimowych. W Polsce grupa Anonymous stała się popularna w 2012 roku, kiedy w związku z głosowaniem nad porozumieniem ACTA (*Anti-Counterfeiting Trade Agreement*) zaczęła atakować strony rządowe, a Polacy wyszli na ulice, by manifestować sprzeciw wobec tej umowy i walczyć o wolność w Internecie. Należy zwrócić uwagę na to, że do najbardziej znanych grup haktywistycznych oprócz Anonymous należą również wcześniej wspomniane Cult of the Dead Cow, Hacktivisimo, Critical Art Ensemble, a także Electronic Disturbance Theater (EDT). Każda z tych grup wsławiła się innymi sposobami działania z wykorzystaniem różnych technik.

TECHNIKI STOSOWANE PRZEZ HAKTYWISTÓW

Głównym celem haktywistów są podmioty, które przyczyniają się do ograniczania wolności, w tym również wolności w Internecie (Chodubski 2014: 130–131), takie jak na przykład państwa, podmioty *quasi*-państwowe i korporacje transnarodowe. Haktywiści,

[6] *The Hactivisimo Declaration*, www.cultdeadcow.com/cDc_files/declaration.html [28.03.2016].

[7] T. McCormick, *Hacktivism: A Short Histor*y, www.foreignpolicy.com/2013/04/29/hacktivism-a-short-history [28.03.2016].

[8] Guy Fawkes (1570–1606) uczestniczył w tzw. spisku prochowym, którego celem była organizacja zamachu na króla Jakuba I. Skutkiem tego miało być przywrócenie katolickiego monarchy na tron. Jednakże spisek został udaremniony, a Fawkesa skazano na śmierć przez powieszenie i poćwiartowanie. Przed wykonaniem wyroku zeskoczył jednak z szafotu i złamał kark, stając się bohaterem m.in. opowieści, książek i filmów. Współcześnie za maskami przypominającymi twarz Fawkesa ukrywają się członkowie grupy Anonymous (Lakomy 2013: 276–277).

wykorzystują nowoczesne technologie, traktując je zarówno jako miejsce walki, jak i broń (Pomarański 2014: 158). Wśród katalogu technik stosowanych przez aktywistów, którzy dążą do realizacji politycznych celów w cyberprzestrzeni, zdaniem Jakuba Nowaka, możemy wyróżnić: *Defacing, Distributed Denial of Service Attacks, Ping Storms, E-mail Bombing, Malicious Code Attacks* i *Redirects* (Nowak 2011: 178). Przechodząc do przykładowych działań, należy zaznaczyć, że w polskiej literaturze badacze bardzo często stosują anglojęzyczne nazwy technik wykorzystywanych przez haktywistów.

Defacing (oszpecenie), określany również jako *Website Defacement*, polega na podmianie zawartości strony internetowej. Jednym z przykładów oszpecenia może być włamanie na stronę internetową syryjskiego rządu i podmiana jej zawartości przez hakera z grupy Teamr00t w odpowiedzi na brak dostępu do Internetu na terenie Syrii w listopadzie 2012 roku. Haktywista zostawił wiadomość dla rządu, w której obarczał Baszara al-Assada odpowiedzialnością za zaistniałą sytuację. Członek grupy Teamr00t domagał się poszanowania praw obywateli do wolności słowa, prowadzenia normalnego życia i dostępu do Internetu. Zapewnił tym samym Syryjczyków, że grupa Teamr00t o nich pamięta i pomoże im odzyskać wolność[9]. Choć syryjski minister informacji przekonywał, że za wyłączenie usług internetowych w kraju odpowiedzialni są rebelianci, haktywiści byli zdania, że winę za te działania ponosi rząd Baszara al-Assada[10].

Jedną z najbardziej powszechnych technik stosowanych przez haktywistów jest *Distributed Denial of Service Attacks* (rozproszona odmowa usługi, DDoS), co oznacza „zaburzenie sieci przez zalanie jej jednoczesnymi pytaniami o dane z tysięcy komputerów" (Nowak 2011: 178). Warto w tym miejscu podać przykład ataku DDoS, który objął sieć internetową w Estonii w kwietniu i maju 2007 roku. Przyczyną ataków były napięte stosunki dyplomatyczne między Estonią a Rosją. Skutki ataków odczuła ta część społeczeństwa, która korzysta z Internetu, tracąc czasowo dostęp do poczty e-mail, bankowości elektronicznej czy innych usług internetowych (Terlikowski 2009: 109–110). Należy wyjaśnić, że atak DDoS jest bardziej skomplikowaną formą ataku DoS (*Dential of Service* – blokada usług). Blokada usług „ma na celu utrudnienie lub przerwanie normalnego działania strony internetowej, serwera lub innego zasobu sieciowego"[11]. Wśród metod należy wyróżnić także *ping storm* (burza ping), nazywaną również *ping flood* (powódź ping). Metodę tę można zaliczyć do prostych ataków DoS. Dla D. Denning ataki DoS/DDoS są przejawami wirtualnego strajku okupacyjnego (*Virtual Sit-In*), którego celem, tak jak w przypadku realnego strajku, jest zwrócenie uwagi na daną kwestię przez blokadę dostępu do określonych obiektów, a co za tym idzie również utrudnianie ich funkcjonowania (Denning 2001: 264). Na tej podstawie można stwierdzić, że technologia zostaje w relatywnie łatwy sposób przystosowana przez społeczeństwo do walki o realizację interesów społeczno-politycznych. W dobie mediów społecznościowych możemy szczególnie zauważyć, że Internet stał się narzędziem

[9] M. Kumar, *#OpSyria: Teamr00t Hack Syrian Government Sites*, www.thehackernews.com/2012/12/opsyria-teamr00t-hack-syrian-government.html [28.03.2016].

[10] *Syria odcięta od świata. Nie działa lotnisko, telefony, Internet*, www.tvn24.pl/wiadomosci-ze-swiata,2/syria-odcieta-od-swiata-nie-dziala-lotnisko-telefony-internet,291653.html [28.03.2016].

[11] *Co to jest atak DoS? Czym jest atak DDoS?*, www.kaspersky.pl/zagrozenia/faq#dos/ddos [03.04.2016].

i płaszczyzną walki politycznej, wprowadzając ją w wymiar, z którym nie mieliśmy nigdy wcześniej do czynienia.

Jeśli w relatywnie krótkim czasie skrzynka e-mail zostaje zapełniona tysiącami wiadomości, w wyniku czego zostaje zablokowana, mamy do czynienia z techniką określaną terminem *e-mail bombing* (Nowak 2011: 178). Na początku kwietnia 2016 roku w Polsce miały miejsce protesty uliczne przeciwko zaostrzeniu ustawy antyaborcyjnej. Ich „przedłużeniem" były również akcje protestacyjne zorganizowane online, między innymi akcja o nazwie „Trudny okres dla rządu" nawiązująca do działań Amerykanek, które sprzeciwiały się zaostrzeniu ustawy antyaborcyjnej w stanie Indiana. Organizatorzy polskiej akcji zachęcali kobiety do częstego i masowego kontaktowania się z premier Beatą Szydło oraz innymi ważnymi osobami i instytucjami za pośrednictwem mediów społecznościowych, telefonów oraz e-maili w celu informowania ich o cyklu menstruacyjnym kobiet czy zasięgania opinii na ten temat. Do wydarzenia na Facebooku przyłączyło się kilka tysięcy osób, jednak dotychczas nie są znane dokładne dane, ile osób faktycznie skontaktowało się w tej sprawie z premier polskiego rządu czy z Konferencją Episkopatu Polski[12]. W czasie oddania artykułu do druku skutki tego typu internetowego protestu nie są jeszcze znane, jednakże jest to jeden z przykładów bombardowania skrzynek e-mailowych rządzących w celu protestu wobec ich działań.

Malicious code attacks (ataki złośliwego oprogramowania), znane również jako *malware*, to wykorzystanie szkodliwych programów komputerowych lub skryptów do zainfekowania podatnych na ataki systemów w celu kradzieży informacji czy uszkodzenia danych[13]. Wśród typów zagrożeń wyróżnia się na przykład wirusy (*viruses*), robaki (*worms*), konie trojańskie (*Trojan*), oprogramowanie szpiegowskie (*spyware*) oraz *rootkity*[14]. Jednym z przykładów wykorzystania ataków szkodliwego oprogramowania było zainfekowanie pierwszej elektrowni atomowej w Iranie robakiem o nazwie Stuxnet. Oprócz elektrowni w Buszerze celem ataków stało się około 30 tysięcy komputerów w tym kraju, również systemy należące do irańskiego przemysłu[15]. Warto zaznaczyć, że Iran został zaatakowany trzykrotnie w okresie od czerwca 2009 do maja 2010 roku. Celem było zablokowanie irańskiego programu atomowego. W efekcie jednego z ataków Stuxnetu odłączonych zostało tysiąc wirówek wzbogacania uranu, w kolejnym natomiast przyśpieszono działanie wirówek, co doprowadziło do ich uszkodzenia[16]. Do dzisiaj nie jest pewne, kto jest twórcą robaka, jednak specjaliści

---

[12] Redakcja, *#TrudnyOkres. Internautki zarzucają Beatę Szydło wieściami o przebiegu swojej... miesiączki*, http://www.polityka.pl/tygodnikpolityka/kraj/1656590,1,trudnyokres-internautki-zarzucaja-beate-szydlo-wiesciami-o-przebiegu-swojej-miesiaczki.read [04.04.2016]; *TRUDNY OKRES dla rządu*, https://www.facebook.com/events/209802169392172 [04.04.2016].

[13] *What is Malicious Code? – Definition*, www.usa.kaspersky.com/internet-security-center/definitions/malicious-code#.VwF_8ZyLTDc [03.04.2016].

[14] *Walka z wirusami: Typy znanych zagrożeń*, www.support.kaspersky.com/pl/viruses/general/614 [03.04.2016].

[15] A. Kazimierczuk, *Cybernetyczny atak na irańską elektrownię atomową*, http://www.rp.pl/artykul/541147-Cybernetyczny-atak-na-iranska-elektrownie-atomowa.html#ap-2 [05.04.2016].

[16] M. Gajewski, *Robak Stuxnet precyzyjnie wymierzony w przemysł Iranu*, http://www.chip.pl/news/wydarzenia/prawo-i-polityka/2011/02/robak-stuxnet-precyzyjnie-wymierzony-w-przemysl-iranu [05.04.2016]. Szerzej na temat ataku: Lakomy M., *Cyberwojna jako rzeczywistość XXI wieku*, http://www.geopolityka.org/analizy/miron-lakomy-cyberwojna-jako-rzeczywistosc-xxi-wieku [05.04.2016].

podejrzewają, że za tak skomplikowanym programem może stać wyłącznie jakieś państwo. Sugeruje się, że za ataki Stuxnetu są odpowiedzialne Izrael oraz Stany Zjednoczone[17].

Redirects (przekierowania) mają miejsce wtedy, kiedy ruch sieciowy jest przekierowany z jednego adresu URL na inny. Technika ta jest powszechnie stosowana, jednak to, czy budzi zagrożenie, czy go nie budzi, zależy od intencji osób dokonujących ataku. Możemy wyobrazić sobie, że na przykład przekierowanie stosowane jest przez osoby, które założyły nową witrynę, ale nie chcą stracić odbiorców, którzy znali stary adres URL strony. Po wpisaniu starego adresu zostają oni przekierowani na nową stronę. Jednak możemy mieć również do czynienia z inną sytuacją, kiedy strona stanie się ofiarą ataku. Wtedy po wpisaniu danego adresu zostajemy przekierowani na inny, na którym na przykład widnieje polityczny manifest lub stajemy się ofiarami szkodliwego oprogramowania. Koncentrując się na technikach, warto zauważyć, że haktywiści wykorzystują również *doxing* (*document tracing*), czyli zbieranie wrażliwych informacji na temat konkretnych osób (imion, nazwisk, adresów zdjęć, zainteresowań) dzięki śledzeniu mediów społecznościowych lub przy użyciu złośliwego oprogramowania. Bardzo często tego typu dane są następnie udostępniane w Internecie lub wykorzystywane przez zleceniodawców do realizacji własnych celów (Füllgraf 2015: 29). Samo zbieranie ogólnodostępnych informacji jest legalne, jednak łatwo można sobie wyobrazić, że zdobyte dane mogą zostać wykorzystane w celu przestępczym. Przykładem zdobywania informacji może być działanie Anonymous po zamachach w Paryżu w 2015 roku. W ramach operacji *#op-Paris* haktywiści zdobyli adresy osób ściśle powiązanych z ISIS, które były odpowiedzialne za rekrutowanie terrorystów. Akcja ta była jednym z elementów walki grupy z ISIS, mającej doprowadzić do likwidacji na Twitterze kont należących do dżihadystów i będących jednym z ich kanałów komunikacji[18].

Wymienione przeze mnie rodzaje technik i ich praktyczne wykorzystanie nie zamykają całego spektrum środków, które mogą być stosowane przez haktywistów. Dzięki możliwościom, jakie niosą nowoczesne technologie, i szybkości zmian, jakim ulegają, haktywiści mogą bardzo szybko reagować na ważne wydarzenia – są w stanie z każdego miejsca globu prowadzić swoje kampanie wymierzone w dowolnie wybrany cel, wykorzystując coraz to nowe sposoby działania. Świadczy o tym reakcja grupy Anonymous na zamachy terrorystyczne w Brukseli w marcu 2016 roku. Po zamachach grupa opublikowała w Internecie oświadczenie, w którym obiecywała wziąć odwet na terrorystach i zachęcała wszystkich Europejczyków do przyłączenia się do działań przeciwko nim. Wszelkim działaniom w ramach tej kampanii towarzyszył specjalny hashtag[19] *#OpBrussels*, co pokazuje, że haktywiści chętnie wykorzystują narzędzia mediów społecznościowych i szybko wdrażają nowe możliwości działania w cyberprzestrzeni[20].

---

[17] mtom, *Stuxnet wymknął się spod kontroli. Zniszczył 100 tys. Komputerów*, http://www.tvn24.pl/internet-hi-tech-media,40/stuxnet-wymknal-sie-spod-kontroli-zniszczyl-100-tys-komputerow,332977.html [08.04.2016].

[18] *Anonymous kontra Państwo Islamskie. Hakerzy publikują dane terrorystów*, http://swiat.newsweek.pl/zamachy-w-paryzu-anonymous-publikuja-dane-panstwa-islamskiego-,artykuly,374144,1.html [07.04.2016].

[19] Hashtagi są tworzone za pomocą symbolu #, za którym znajduje się słowo, np. #haktywizm. Ich celem jest ułatwienie wyszukiwania informacji dzięki ich kategoryzacji. Szerzej na ten temat: M. Nowak, *Komunikacja w kratkę, czyli o hashtagach*, http://www.wirtualnemedia.pl/artykul/komunikacja-w-kratke-czyli-o-hashtagach [06.04.2016].

[20] *Anonymous grożą dżihadystom. „Każdy Europejczyk może włączyć się w tę walkę"*, http://tvn24bis.pl/ze-swiata,75/zamachy-w-brukseli-anonymous-grozi-dzihadystom,629989.html [28.03.2016].

W niniejszej pracy należy uwzględnić również reakcje polskiego rządu na działania haktywistów. W tym celu poddano szczegółowej analizie *Raporty o stanie bezpieczeństwa w Polsce* przygotowane przez MSW (lub MSWiA)[21] w latach 2008–2014 oraz *Raporty o stanie bezpieczeństwa cyberprzestrzeni RP* w latach 2010–2014 przygotowywane przez Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT). Raporty przygotowane przez MSW w latach 2008–2013 nie zawierają żadnych informacji o haktywizmie, dopiero w 2014 roku pojawia się krótka wzmianka na ten temat[22]. Raporty CERT w latach 2010–2011 i 2014 nie poświęciły uwagi haktywizmowi, natomiast w 2012 i 2013 roku wymieniają szczegółowe wydarzenia, jakie miały miejsce w tych latach i zostały zorganizowane przez haktywistów. Dla przykładu warto podać, że w 2013 roku odnotowano wiele podmian witryn internetowych należących między innymi do Ministerstwa Edukacji Narodowej, Sądu Rejonowego w Wieluniu i Sądu Okręgowego we Wrocławiu[23]. Twórcy raportu z 2013 roku zauważają, że podmiany witryn były związane z propagowaniem idei politycznych lub zwykłą dewastacją wizerunku strony. Nasuwa się więc pytanie, czy w Polsce haktywizm istotnie nie jest zagrożeniem? W świetle dotychczasowych wyników badań trudno znaleźć jednoznaczną odpowiedź na to pytanie.

SPOŁECZNE KORZYŚCI I ZAGROŻENIA

Z dotychczasowych rozważań wynika, że haktywizm ma różne oblicza. Nie ulega wątpliwości, że ze względu na swą złożoność i niejednorodność ma wielu zwolenników

[21] Autorem raportów jest ministerstwo właściwe do spraw wewnętrznych. Zmieniający się autor raportu wynika ze zmian nazwy ministerstwa i przysługujących mu kompetencji.

[22] MSWiA, *Raport o stanie bezpieczeństwa w Polsce w 2008 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016]; MSWiA, *Raport o stanie bezpieczeństwa w Polsce w 2009 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016]; MSWiA, *Raport o stanie bezpieczeństwa w Polsce w 2010 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016], MSW, *Raport o stanie bezpieczeństwa w Polsce w 2011 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016]; MSW, *Raport o stanie bezpieczeństwa w Polsce w 2012 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016]; MSW, *Raport o stanie bezpieczeństwa w Polsce w 2013 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016]; MSW, *Raport o stanie bezpieczeństwa w Polsce w 2014 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016].

[23] CERT, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku*, *http*://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/422,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2010-roku.html [04.04.2016]; CERT, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/549,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2011-roku.html [04.04.2016]; CERT, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/605,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2012-roku.html [04.04.2016]; CERT, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/686,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2013-roku.html [04.04.2016]; CERT, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html [04.04.2016].

i przeciwników. W literaturze wskazuje się również na wiele szans i zagrożeń, jakie niesie ze sobą ten rodzaj aktywności zarówno dla społeczeństwa, jak i struktur państwa. Należy podkreślić, że jest to niezwykle wymagający obszar badawczy – istnieje relatywnie mało wyników badań na ten temat i dlatego badacze bazują głównie na tych samych źródłach. Ponadto przynależność do grup haktywistycznych jest nieformalna, w związku z tym miarodajne określenie na przykład socjoekonomicznych cech członków grup może stanowić trudność.

Jak wynika z przeprowadzonych badań, dwa główne nurty haktywizmu (elektroniczne nieposłuszeństwo obywatelskie i haktywizm informacyjny) prezentują pewne uniwersalne postulaty. Haktywiści walczą między innymi o prawa człowieka, wartości demokratyczne, dostęp do informacji czy niezakłócony dostęp do Internetu, które szerzej wiążą się z kwestią wolności. Grupy haktywistów bronią tym samym uniwersalnych zasad zapisanych między innymi w Deklaracji Praw Człowieka. M. Lakomy twierdzi, że haktywiści na ogół nie dokonują poważnych zniszczeń i nie stanowią dużego zagrożenia dla bezpieczeństwa państwa, ponieważ ich działania mają na celu przykucie uwagi opinii publicznej do danej kwestii czy zainicjowania debaty na dany temat (Lakomy 2015: 145). Uzupełnieniem mogą być również wyniki badań M. Terlikowskiego, który dochodzi do wniosku, że ataki dokonywane przez pojedyncze osoby mają ograniczone skutki i relatywnie małą skalę, przez co zazwyczaj wpływają na straty wizerunkowe danego celu (Terlikowski 2009: 110). Tego typu działania mogą skutkować na przykład stratami finansowymi dla korporacji, a dla państwa osłabieniem pozycji negocjacyjnej rządu w trakcie negocjacji międzynarodowych. Dużo większym zagrożeniem, zdaniem Terlikowskiego, jest działanie, które paraliżowałoby funkcjonowanie całej sieci Internet w danym państwie, ponieważ z możliwości Internetu korzysta wiele podmiotów (na przykład sektor finansowy, administracja państwowa, osoby prywatne), a ponadto z Internetem mogą być ściśle sprzężone inne systemy teleinformatyczne (Terlikowski 2009: 110). Jednakże, jak już zostało wcześniej ukazane, te same zjawiska mogą być różnie interpretowane zarówno przez badaczy, jak i przez opinię publiczną. Jedni będą je utożsamiali z niegroźnymi dla bezpieczeństwa przejawami haktywizmu, inni natomiast z poważnym zagrożeniem pod postacią cyberterroryzmu.

Szczegółowa analiza problemu wskazuje, że często działalność haktywistów w Internecie jest niejako przedłużeniem protestów i manifestacji, które mają miejsce w życiu realnym. Może to skutkować wzbogaceniem życia społeczno-politycznego i przynieść pozytywne rezultaty dla rozwoju społeczeństwa obywatelskiego. Walka o wolny dostęp do informacji i jej wymianę może natomiast zwiększać świadomość ludzi na temat aktualnej sytuacji politycznej lub gospodarczej, niezależnie od tego, które treści są wynoszone na agendę przez rządzących. Haktywiści mają udział w nagłaśnianiu kwestii, które z różnych względów rządzący próbują maskować. Było to widoczne w przypadku działań Anonymous i protestów społeczeństwa przeciwko uchwaleniu ACTA. Na tym przykładzie możemy zobaczyć zatem, że haktywizm może stanowić swoisty wentyl bezpieczeństwa, mobilizować ludzi wokół konkretnego problemu i chronić społeczeństwo przed nadużyciami władzy. Ponadto w pewnych granicach i przy użyciu odpowiednich narzędzi Internet jest w stanie zapewnić ludziom anonimowość, pozwala wyrażać poglądy, które mogą być niepopularne z linią rządzących.

Należy przy tym zwrócić uwagę na fakt, że rządzący boją się potencjału, jaki niosą ze sobą nowoczesne technologie, w tym media społecznościowe, a tym samym interesujące jest

to, jak nowy wymiar usieciowienia społeczeństwa może wpływać na władzę. Manuel Castells w książce poświęconej ruchom społecznym w dobie Internetu pokazuje reakcję państwa na rewolucję internetową na przykładzie wydarzeń w Egipcie. Rząd egipski w 2011 roku podjął próbę blokady portali społecznościowych w Internecie ze względu na to, że to właśnie tam nawoływano do protestów i na bieżąco informowano na temat wydarzeń mających miejsce na placu Tahrir. Nie przyniosło to zamierzonego skutku, dlatego rządzący posunęli się do bardziej restrykcyjnych działań: na żądanie egipskiego rządu najwięksi operatorzy w nocy 27 i 28 stycznia 2011 roku zablokowali połączenia internetowe. W rezultacie w skali całego kraju ruch internetowy został zablokowany w 93%. Powyższe dane pozwalają stwierdzić, że rządowi nie udało się doprowadzić do całkowitego odcięcia dostępu do Internetu – podczas blokady usługi internetowe świadczyli mniejsi operatorzy, mający siedziby głównie w ośrodkach akademickich (Castells 2013: 71–72).

Blokada Internetu w kraju potrwała kilka dni. Wiele czynników złożyło się na to, że mieszkańcom udało się ją przezwyciężyć. Co ważne, brak Internetu nie oznaczał dla protestujących braku kontaktu ze sobą nawzajem oraz ze społecznością międzynarodową. Odcięcie od Internetu udało się obejść, a największą rolę w tych dniach odegrały czynniki, o których wspomina M. Castells. Istotna była działalność telewizji Al-Dżazira, która uzyskiwała informacje i obrazy od zaangażowanych osób dzięki połączeniom telefonicznym i ułatwiała rozprzestrzenianie się wiadomości. Egipcjanie wykorzystywali ponadto inne kanały komunikacji – faksy, krótkofalówki czy modemy telefoniczne. Wsparcia w tych działaniach udzielili im zagraniczni dostawcy usług internetowych, a także inżynierowie pracujący dla Google'a i Twittera – okrężnymi sposobami, wykorzystując połączenia z telefonów stacjonarnych oraz możliwości programu, który automatycznie przekształcał wiadomości nagrane na poczcie głosowej i publikował je jako wpisy na Twitterze (tak zwane tweety). Dodatkowo hakerzy zgrupowani w międzynarodowej organizacji Telecomix przygotowali program automatycznie pobierający wiadomości telefoniczne i wysyłający je w formie faksów w Egipcie. Ponadto wykorzystano amatorskie radia nadające na określonych częstotliwościach. Osoby znające się na sposobach ominięcia cenzury przyczyniły się również do powstania ulotek z informacjami dotyczącymi możliwości komunikowania się pomimo blokady Internetu, które następnie rozdawano wśród protestujących (Castells 2013: 72–74). Te i wiele innych czynników doprowadziły do tego, że 1 lutego 2011 roku przywrócono dostęp do Internetu. Według wyliczeń dokonanych przez Organizację Współpracy Gospodarczej i Rozwoju (*Organisation for Economic Co-operation and Development*, OECD) pięciodniowa blokada usług internetowych i telekomunikacyjnych przyniosła Egiptowi straty w wysokości 90 milionów dolarów, a łączne straty wyniosły około 3–4% egipskiego PKB. Przy czym należy podkreślić, że dane te nie uwzględniają strat finansowych, jakie dotknęły firmy funkcjonujące w innych sektorach gospodarki, między innymi w branży turystycznej czy handlu elektronicznym (Castells 2013: 75). M. Castells uważa, że głównym powodem przywrócenia dostępu do Internetu był fakt, że blokada nie powstrzymała ludzi od protestów. Autor podkreśla również, że blokada została zastosowana zbyt późno, by mogła zdusić działania ruchu. Ludzie protestowali na ulicach, a świat był poinformowany o egipskiej rewolucji. Ponadto Egipcjanie stosowali inne, autonomiczne metody komunikacji, protesty opierały się nie tylko na sieciach internetowych, ale również na bezpośrednich sieciach istniejących w realnym życiu, stąd działania rządu nie przyniosły oczekiwanych rezultatów (Castells 2013: 75–76).

Rezultaty badań wskazują również na to, że techniki, które stosują haktywiści, są nie do końca legalne lub całkowicie nielegalne. Przykładem może być *e-mail bombing*, który jedni badacze zaliczają do haktywizmu, inni zaś do cyberterroryzmu. Kolejny problem dotyczy legitymizacji działań: w ulicznych protestach legitymizację nadaje liczebność tłumu. W przypadku akcji mających miejsce online bardzo trudno jest udowodnić, że za konkretnym działaniem stoi duża grupa ludzi, a nie jeden człowiek, który za sprawą kliknięcia i odpowiedniego programu dokonuje ataku (Jordan 2011: 91–92). Haktywizm rodzi zagrożenie również z powodu braku formalnej przynależności do grup. W rezultacie nie istnieje jednoznaczna hierarchia i podległość służbowa, a struktury są zdecentralizowane. Może to powodować, że niektórzy indywidualni haktywiści będą dokonywali ataków samodzielnie, pod wpływem chwili i emocji, bez konsultacji z pozostałymi członkami grupy i bez ich zgody na takie działania, co może mieć również poważne konsekwencje. Kolejną kwestią, którą warto rozważyć, jest stopień motywacji haktywistów – w przypadku wysokiego stopnia motywacji haktywiści mogą być zdeterminowani do coraz trudniejszych działań, stając się przez to nieprzewidywalni. Warto zaznaczyć, że aby zostać haktywistą, nie trzeba posiadać specjalistycznej wiedzy na temat programowania i nowych technologii, wystarczy dysponować odpowiednimi środkami pieniężnymi, by walczyć o realizację celów politycznych w cyberprzestrzeni, na przykład zlecając wykonanie specjalistycznych programów lub ataków innej osobie. M. Terlikowski zwraca uwagę na to, że możliwe jest, by zmotywować osobę, która dysponuje szczególnie dużą wiedzą informatyczną, do przeprowadzenia jednoczesnego ataku nie tylko na Internet, ale również na inne systemy teleinformatyczne – co byłoby większym zagrożeniem dla bezpieczeństwa niż zwykłe działania haktywistów (Terlikowski 2009: 109).

Współcześnie, ze względu na szybki postęp technologiczny i nadmiar informacji, trudno jest weryfikować docierające do nas wiadomości. Używanie specjalistycznych narzędzi może umożliwić ludziom o dobrych intencjach zachowanie anonimowości w obawie przed represjami rządu. Jednakże możemy sobie wyobrazić również sytuację, w której za pomocą narzędzi pozwalających zakamuflować źródło działania pod haktywistów podszywają się agenci służb specjalnych obcych krajów – szkodząc wizerunkowi ruchu haktywistycznego, a także interesom państwa. Ponadto haktywiści mogą mieć dobre intencje, ale efekty ich działań mogą wykorzystywać osoby będące zagrożeniem dla państwa i społeczeństwa.

ZAKOŃCZENIE

Haktywiści stosują metody wywodzące się z hakerstwa, a główna cecha, która ich rozróżnia, to polityczna motywacja. Jak twierdzi M. Castells, „Internet zapewnia organizacyjną platformę komunikacji, dzięki której kultura wolności przekłada się na praktykę autonomii" (Castells 2013: 221). Autor podkreśla przy tym, że Internet został stworzony przez naukowców i hakerów jako obszar pozbawiony centralnej władzy, będący zdecentralizowaną siecią komunikacji. To spostrzeżenie może wzbogacić nasze spojrzenie na fenomen haktywizmu. Do tego należy dodać za Castellsem, że w XXI wieku nastąpiła społeczna przemiana Internetu – kontakty indywidualne i biznesowe, których uosobieniem było korzystanie z poczty elektronicznej, zostały zastąpione autonomiczną konstrukcją sieci społecznościowych,

kształtowanych przez użytkowników (Castells 2013: 221–222). Zmiany te niepostrzeżenie wpłynęły również na haktywistów i ich działania w Internecie.

Celem artykułu była ocena haktywizmu pod kątem szans i zagrożeń, jakie niesie ze sobą to zjawisko. Szukano w nim odpowiedzi na pytanie badawcze, czy haktywizm jest społeczną korzyścią, czy zagrożeniem. Podsumowując dotychczasowe rozważania, należy stwierdzić, że to pytanie wydaje się na tym etapie badań nierozstrzygalne. Największa trudność tkwi w szerokiej definicji haktywizmu i braku jednoznacznego odróżnienia tego zjawiska od innych mających miejsce w cyberprzestrzeni. Warto odnotować, że wiele cech haktywizmu powoduje, że możemy je interpretować zarówno jako szanse, jak i zagrożenia. Dla przykładu warto podać, że haktywiści stawiają na bezpośrednie akcje, dzięki temu w działalność grupy może włączyć się prawie każdy, w tym również osoby, które nie mają specjalistycznej wiedzy. Ma to zarówno skutki pozytywne – umożliwia aktywny udział w życiu grupy i współuczestniczenie w proteście każdemu człowiekowi, jak i negatywne – niektórzy mogą podszywać się pod członków grupy, szkodząc nie tylko jej wizerunkowi, ale przyczyniając się do powstawania poważnych zagrożeń. Z wielu powodów politycy obawiają się haktywistów, ponieważ nie do końca są w stanie poznać to środowisko. Jedni widzą w haktywizmie zagrożenie ze względu na rozluźnianie więzi społecznych, inni natomiast uważają, że może on stanowić korzyść, przeciwdziałając dehumanizacji społeczeństwa.

Współcześnie w Polsce haktywizm jest jeszcze ruchem mało wyraźnym, w publicznej dyskusji i potocznym rozumieniu utożsamianym z innymi zjawiskami. Przewiduje się natomiast, że w perspektywie najbliższych lat haktywizm będzie się rozwijał, próbując zwiększyć swój wpływ na decyzje rządzących. Trudno jest jednak jednoznacznie wskazać konkretnie kierunek rozwoju tego ruchu. Warto przy tym zaznaczyć, że w ostatnich latach wzrasta zainteresowanie haktywizmem nie tylko wśród badaczy, ale również wśród twórców literatury popularnej. Rozwój haktywizmu i wzrost zainteresowania tą tematyką powinien być związany ze zwiększającą się świadomością i wiedzą społeczeństwa na temat technik haktywizmu oraz szans i zagrożeń, jakie dzięki nim powstają. Zapewnienie bezpieczeństwa oraz przeciwdziałanie nielegalnym technikom stosowanym przez haktywistów wymaga współpracy państw. Niniejszy artykuł nie zamyka zatem refleksji nad zjawiskiem haktywizmu, lecz otwiera na nowe obszary badawcze, stanowiąc tym samym punkt wyjścia do interdyscyplinarnych badań nad różnymi jego odcieniami.

BIBLIOGRAFIA

Castells, Manuel. 2013. *Sieci oburzenia i nadziei. Ruchy społeczne w erze Internetu.* Warszawa: Wydawnictwo Naukowe PWN, s. 71–222.

Chodubski, Andrzej. 2014. *Haktywizm jako zjawisko polityczne w cywilizacji informacyjnej*, w: Maria Marczewska-Rytko (red.). *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja)*, Lublin: Wydawnictwo UMCS, s. 125–138.

Denning, Dorothy. 2001. *Activism, Hacktivism and Cyberterrorism. The Internet as a Tool for Influencing*, w: John Arquilla i David Ronfeldt (red.). *Networks and Netwars. The Future of Terror, Crime and Militancy*, Santa Monica: RAND Corporation, s. 239–288.

du Vall, Marta i Marta Majorek. 2013. *Nowe media w służbie „sieciowych" aktywistów*, w: Małgorzata Wysocka-Pleczyk i Barbara Świeży (red.). *Człowiek zalogowany 1.*

Od mowy nienawiści do integracji w sieci, Kraków: Biblioteka Jagiellońska, [online:] jbc.bj.uj.edu.pl, s. 27–37.

Jordan, Tim i Paul Taylor. 2004. *Hacktivism and Cyberwars. Rebels with a cause?*, London: Routledge.

Jordan, Tim. 2011. *Hakerstwo*, Warszawa: Wydawnictwo Naukowe PWN.

Jordan, Tim. 2016. *A genealogy of hacking*, „Convergence: The International Journal of Research into New Media Technologies", 1–17.

Lakomy, Mirosław. 2013. *Demokracja 2.0. Interakcja polityczna w nowych mediach*, Kraków: Wydawnictwo WAM.

Lakomy, Mirosław. 2015. *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice: Uniwersytet Śląski.

Macała, Jarosław. 2014. *Grupa Anonymous: cyberprzestępcy czy rycerze wolności? Polskie echa*, w: Maria Marczewska-Rytko (red.). *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja)*, Lublin: Wydawnictwo UMCS, s. 189–202.

Nowak, Jakub. 2011. *Aktywność obywateli online. Teorie a praktyka*, Lublin: Wydawnictwo UMCS.

Pomarański, Marcin. 2014. *Haktywizm jako ruch protestu XXI wieku*, w: Maria Marczewska-Rytko (red.). *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja)*, Lublin: Wydawnictwo UMCS: 153–168.

Samuel, Alexandra. 2004. *Hacktivism and the Future of Political Participation* [niepublikowana rozprawa doktorska], http://alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf [04.04.2016].

Terlikowski, Marcin. 2009. *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*, w: Marek Madej i Marcin Terlikowski (red.). *Bezpieczeństwo teleinformatyczne państwa*, Warszawa: Polski Instytut Spraw Międzynarodowych, s. 95–122.

RAPORTY

CERT. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/422,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2010-roku.html [04.04.2016].

CERT. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/549,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2011-roku.html [04.04.2016].

CERT. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/605,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2012-roku.html [04.04.2016].

CERT. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/686,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2013-roku.html [04.04.2016].

CERT. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html [04.04.2016].

Füllgraf, Wendy. 2015. *Abschlussbericht zum Projektteil der Hellfeldbeforschung*, Bundeskriminalamt Kriminalistisches Institut Forschungs- und Beratungsstelle Cybercrime KI 16, https://netzpolitik.org/wp-upload/2015HacktivistenProjektteilHellfeldbeforschung.pdf [07.04.2016].

MSW. *Raport o stanie bezpieczeństwa w Polsce w 2011 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016].

MSW. *Raport o stanie bezpieczeństwa w Polsce w 2012 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016].

MSW. *Raport o stanie bezpieczeństwa w Polsce w 2013 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016].

MSW. *Raport o stanie bezpieczeństwa w Polsce w 2014 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016].

MSWiA. *Raport o stanie bezpieczeństwa w Polsce w 2008 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016].

MSWiA. *Raport o stanie bezpieczeństwa w Polsce w 2009 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016].

MSWiA. *Raport o stanie bezpieczeństwa w Polsce w 2010 roku*, http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html [03.04.2016].

ŹRÓDŁA INTERNETOWE

Anonymous grożą dżihadystom. „Każdy Europejczyk może włączyć się w tę walkę”, http://tvn24bis.pl/ze-swiata,75/zamachy-w-brukseli-anonymous-grozi-dzihadystom,629989.html [28.03.2016].

Anonymous kontra Państwo Islamskie. Hakerzy publikują dane terrorystów, http://swiat.newsweek.pl/zamachy-w-paryzu-anonymous-publikuja-dane-panstwa-islamskiego-,artykuly,374144,1.html [07.04.2016].

Co to jest atak DoS? Czym jest atak DDoS?, www.kaspersky.pl/zagrozenia/faq#dos/ddos [03.04.2016].

Critical Art Ensemble. *Electronic Civil Disobedience & Other Unpopular Ideas*, http://www.critical-art.net/books/ecd [04.04.2016].

Gajewski, Maciej. *Robak Stuxnet precyzyjnie wymierzony w przemysł Iranu*, http://www.chip.pl/news/wydarzenia/prawo-i-polityka/2011/02/robak-stuxnet-precyzyjnie-wymierzony-w-przemysl-iranu [05.04.2016].

Hauben, Michael. *The Net and Netizens: The Impact the Net has on People's Lives*, http://www.columbia.edu/~rh120/ch106.x01 [05.04.2016].

Kazimierczuk, Agnieszka. *Cybernetyczny atak na irańską elektrownię atomową*, http://www.rp.pl/artykul/541147-Cybernetyczny-atak-na-iranska-elektrownie-atomowa.html#ap-2 [05.04.2016].

Kumar, Mohit. *#OpSyria: Teamr00t Hack Syrian Government Sites*, http://www.thehackernews.com/2012/12/opsyria-teamr00t-hack-syrian-government.html [28.03.2016].

Lakomy, Mirosław, *Cyberwojna jako rzeczywistość XXI wieku*, http://www.geopolityka.org/analizy/miron-lakomy-cyberwojna-jako-rzeczywistosc-xxi-wieku [05.04.2016].

McCormick, Ty. *Hacktivism: A Short History*, http://foreignpolicy.com/2013/04/29/hacktivism-a-short-history [28.03.2016].

mtom, *Stuxnet wymknął się spod kontroli. Zniszczył 100 tys. komputerów*, http://www.tvn24.pl/internet-hi-tech-media,40/stuxnet-wymknal-sie-spod-kontroli-zniszczyl-100-tys-komputerow,332977.html [08.04.2016].

Nowak, Mikołaj. *Komunikacja w kratkę, czyli o hashtagach*, http://www.wirtualnemedia.pl/artykul/komunikacja-w-kratke-czyli-o-hashtagach [06.04.2016].

Redakcja, *#TrudnyOkres. Internautki zarzucają Beatę Szydło wieściami o przebiegu swojej... miesiączki*, http://www.polityka.pl/tygodnikpolityka/kraj/1656590,1,trudnyokres-internautki-zarzucaja-beate-szydlo-wiesciami-o-przebiegu-swojej-miesiaczki.read [04.04.2016].

Święcicka, Olga. *Generacja leni – slaktywiści. Czy można zbawić świat, klikając myszką?*, http://natemat.pl/34501,generacja-leni-slaktywisci-czy-mozna-zbawic-swiat-klikajac-myszka [06.04.2016].

Syria odcięta od świata. Nie działa lotnisko, telefony, Internet, http://www.tvn24.pl/wiadomosci-ze-swiata,2/syria-odcieta-od-swiata-nie-dziala-lotnisko-telefony-internet,291653.html [28.03.2016].

Tajemnicze przestępstwa w sieci, http://technowinki.onet.pl/militaria/tajemnicze-przestepstwa-w-sieci/4kl7s [05.04.2016].

The Hactivisimo Declaration, www.cultdeadcow.com/cDc_files/declaration.html [28.03.2016].

Trudny okres dla rządu, https://www.facebook.com/events/209802169392172 [04.04.2016].

Walka z wirusami: Typy znanych zagrożeń. www.support.kaspersky.com/pl/viruses/general/614 [03.04.2016].

What is Malicious Code? – Definition, www.usa.kaspersky.com/internet-security-center/definitions/malicious-code#.VwF_8ZyLTDc [03.04.2016].

IS HACKTIVISM A SOCIAL BENEFIT OR THREAT?

This article focuses on the theme of hacktivism, which is a marriage of the world of technology and the world of politics. Hacktivism is a combination of socio-political activism and hacking. The research problem of this article is the question, is hacktivism a social benefit or a threat? The main thesis is that hacktivism is not serious threat to the society and the state structures. The article provides an overview of the most important definitions of hacktivism and hacktivists' techniques with the examples of the 21st century. It also attempts to assess this phenomenon in terms of the opportunities and threats posed to citizens and state institutions, and presents the projected direction of this development.

Keywords: hacktivism, electronic civil disobedience