

MAŁGORZATA WYSOCKA-PLECZYK  
BEATA ŚWIEŻY

---

# CZŁOWIEK ZALOGOWANY



**1** OD MOWY NIENAWIŚCI  
DO INTEGRACJI W SIECI

MAŁGORZATA WYSOCKA-PLECZYK  
BEATA ŚWIEŻY

---

# CZŁOWIEK ZALOGOWANY

**1** OD MOWY NIENAWIŚCI  
DO INTEGRACJI W SIECI

Redakcja techniczna:

Małgorzata Wysocka-Pleczyk

Projekt okładki:

Mira Pikor

Recenzja:

dr Kinga Tucholska

Treść książki jest udostępniona na licencji Creative Commons – Uznanie autorstwa – Na tych samych warunkach 3.0 (CC-BY-SA) dostępnej pod adresem <http://creativecommons.org/licenses/by-sa/3.0>.

ISBN 978-83-934926-4-0

Kraków, 2013

Biblioteka Jagiellońska

Marta du Vall, Marta Majorek

## Nowe media w służbie „sieciowych” aktywistów

### Wstęp

Obecnie żyjemy w epoce toczącej się rewolucji informacyjnej, której wyznacznikiem jest imponujący rozwój form interaktywnej partycypacji jednostek. Nie ulega wątpliwości, że zjawisku temu sprzyja rozwój nowych mediów<sup>1</sup>, które zmieniły krajobraz medialny w znaczącym stopniu i wpływają na tworzenie nowych strategii komunikacyjnych oraz obszarów dialogu społecznego. Można stwierdzić, że obecnie mamy do czynienia z „kulturą nowych mediów”, a internet stanowi swego rodzaju „autostradę informacyjną” (Jaskiernia, 2006). Wśród głównych przejawów rewolucji informacyjnej wymienia się interaktywność, czyli relację między jednostką a środowiskiem, zapośredniczoną przez dane medium<sup>2</sup>. Uzyskując status uczestnika mediów odbiorca współtworzy je, co w dalszym etapie pozwala osiągnąć przez niego pozycję nadawcy. Kolejnym elementem jest hipertekstowość, definiowana jako interaktywny dostęp do wszystkich danych z każdego miejsca na świecie. Podobnie, jak cyfryzacja stanowi szeroko wykorzystywany sposób tworzenia treści, tak samo hipertekstowość staje się formą jej przechowywania oraz przekazywania. W kontekście rewolucji informacyjnej nie należy również pominąć kwestii komunikacyjności. Sieć w sposób naturalny wychodzi naprzeciw naturalnej formie ludzkiej aktywności, jaką jest interakcja. Komunikacyjny wymiar sieci polega na tym, że umożliwia jednostkom, a wręcz zachęca je do wnoszenia ich własnego wkładu w zbiorowe medium. W efekcie, zarówno procesy informacyjne, jak i powstający wokół nich rodzaj organizacji społecznej przybierają jednocześnie charakter zbiorowy, jak i indywidualny. Dla porównania, obcowanie z książką sprzyja raczej indywidualnemu rozwojowi jednostki, w pewnym sensie izoluje ją od otoczenia i nie stwarza możliwości ingerencji w swoją treść. Sieć internetowa natomiast, w związku ze swoją otwartością, umożliwia włączenie się w globalny obieg informacji, dając jednocześnie szansę wprowadzenia nowych treści w czasie rzeczywistym. Ma to niebagatelne znaczenie, jeżeli wziąć pod uwagę przyspieszenie wzrostu ludzkiej produkcji intelektualnej (de Kerckhove, 2001).

Charakterystyczne dla epoki rewolucji informacyjnej zjawisko komunikacji zapośredniczonej, zmediatyzowanej, sprzyja kreowaniu konstrukcji społeczeństwa medialnego (*mediated society*). W obrębie tego terminu zawiera się zarówno pojęcie społeczeństwa informacyjnego (co do treści), jak i społeczeństwa sieciowego w aspekcie formy (Goban-Klas, 2005). Aspekt formalny jest tutaj mocno eksponowany, jednakże nie można doszukać się jakiegokolwiek gradacji w obrębie tej formuły: sieć, informacja, forma i treść mają znaczenie równorzędne i powiązane są ściśle łańcuchem wzajemnych relacji. Nowa formacja społeczna, jaka wyłania się w rezultacie procesów „mediamorfozy”, czyli wysycenia, a raczej nawet przesylenia społeczeństwa mediami, wykazuje kilka znamienych elementów. Przede wszystkim jego dominującą cechą staje się funkcjonowanie w sposób niebezpośredni kontaktów interpersonalnych, w związku z czym media stają się w pewnym sensie „naturalnym” środowiskiem człowieka, a wirtualna przestrzeń staje się powoli równoznaczna z rzeczywistością. Infrastruktura globalna, zwłaszcza w obszarze telekomunikacyjnym przekształca się powoli w fundament sieci i obiegów informacyjnych w wysoce zróżnicowanej skali, począwszy od lokalnej, a na globalnej skończywszy (Goban-Klas, 2005).

<sup>1</sup> Nowe media najczęściej definiuje się jako przekaz cyfrowy.

<sup>2</sup> W tym wypadku będziemy mieć na uwadze zwłaszcza media określane mianem „nowych” bądź te, które określamy jako „stare” lecz uzbrajamy je w narzędzia interaktywne.

Zarysowany pokrótce wpływ nowych technologii na rozwój społeczeństwa informacyjnego i wzrost możliwości nieskrępowanego uczestnictwa jednostek w przestrzeni publicznej stanowi podstawę dla rozważań dotyczących współczesnych form partycypacji. Przedmiotem rozważań autorek są nowe możliwości działania i nowe przestrzenie, jakie kreują dla nich nowe media.

### **Internet jako narzędzie partycypacji w życiu publicznym**

W licznych badaniach, jakie podejmują problematykę relacji pomiędzy korzystaniem z nowych technologii, w tym wypadku głównie z internetu, a poziomem aktywności, wiedzy i rzeczywistej partycypacji w życiu publicznym, wyodrębnić można dwa główne podejścia (Kenski, Stroud, 2006). Zaznaczyć należy, iż ich zwolennicy prezentują przeciwstawne punkty widzenia. Po jednej stronie odnajdziemy tych, którzy stoją na stanowisku, iż korzystanie z nowych technologii w żaden sposób nie ma związku ze zjawiskiem uczestnictwa. Wspierają się oni argumentacją, iż jednostki, które czerpią wiedzę na tematy polityczne z internetu, w przeważającej większości zaliczyć można do grupy już aktywnej politycznie, bądź zainteresowanej polityką na tyle, że dostęp do internetu nie wpływa w istotny sposób na zwiększenie wśród nich poziomu politycznego uczestnictwa. Dodać należy, że nie powinno się oczekiwać, od jednostek nie przejawiających jakiegokolwiek zainteresowania polityką, że będą poszukiwać w internecie informacji z tej dziedziny. W związku z tym, uprawnione wydaje się założenie, zgodnie z którym aktualny poziom wiedzy o polityce oraz uczestnictwa politycznego w danym społeczeństwie, nawet mimo zwiększania się dostępności internetu, nie przejawia zauważalnych tendencji wzrostowych. W bardziej skrajnym wydaniu, internet w pewnej mierze stwarza niebezpieczeństwo dla partycypacji i wywiera na nią zgubny wpływ, sprzyjając zamykaniu się jednostek w kręgu spraw prywatnych i ograniczając ich interakcje z innymi wyłącznie do wymiaru towarzyskiego (Wojniak, 2010b).

Przeciwnie, „optymistyczne” przekonanie przejawia natomiast stosunkowo liczna grupa znawców tematu, dla których zasadne będzie twierdzenie, iż korzystanie z nowości technologicznych w mniej lub bardziej bezpośredni sposób zwiększa poziom zaangażowania w sprawy publiczne. W ich opinii internet wzmacnia polityczną skuteczność, podnosi poziom wiedzy na tematy polityczne, co w dalszej kolejności pozytywnie wpływa na poziom i intensywność jednostkowej partycypacji. Abstrahując od roli źródła informacji o istotnych z punktu widzenia społeczeństwa zagadnieniach politycznych, kandydatach w bieżącej kampanii wyborczej lub działalności władzy ustawodawczej czy wykonawczej, internet to niewątpliwie medium wydatnie ułatwiające kontakt z politykami i jednocześnie dające obywatelom poczucie sprawowania kontroli nad ich działaniami. Znaczenie niewątpliwie ma również fakt, iż specyfika internetu sprawia, że jednostki nie czują się zakłopotane swoim brakiem obeznania i niewiedzą w obszarze polityki (Wojniak, 2010b). Należy uznać, że wzrost dostępności do medium jakim jest internet oraz podniesienie poziomu edukacji, nie tylko tej technologicznej, wpływają na większy poziom partycypacji publicznej obywateli. Warto zauważyć równocześnie fakt, iż internet stwarza nowe możliwości korzystania z wolności osobistych i politycznych. Zwolennicy wpływu technologii informacyjnej na demokrację są przekonani, że uchroni to świat przed kolejnymi dyktaturami, tworzeniem zamkniętych społeczeństw. Można powiedzieć, że demokracja w społeczeństwie informacyjnym to przede wszystkim możliwość świadomego wyboru. To okazja do stanowienia o sobie, podejmowania decyzji w zgodzie z samym sobą (du Vall, 2010).

### **Haktywizm – protest w środowisku sieciowym**

Wszystkie zjawiska opisywane powyżej pozwalają nam dziś obserwować wzrost liczebności i tym samym aktywności grup, które obrały sobie internet za podstawowe narzędzie i zarazem główne pole

działania. Potencjał stwarzany przez nowe technologie jest wykorzystywany zarówno przez organizacje z pogranicza legalnej polityki, jak i struktury z głównego nurtu życia politycznego. Z tego też względu w obrębie form politycznego uczestnictwa obywateli zaobserwować można istotne modyfikacje. Przed jednostkami otwierają się szersze przestrzenie zaangażowania, pojęcie obywatela zyskuje nieco inny wymiar: z jednostki, która ogranicza się do użytkowania i dokonywania wyborów w przestrzeni publicznej (*users and choosers*) zaczyna być utożsamiany z podmiotem kreującym i nadającym jej pożądany przez siebie kształt. Nie zawsze jednak istnieją instytucje i mechanizmy, które w sposób ogólnie przyjęty (dozwolony) na to pozwalają i podówczas otwiera się pole dla działalności, która poza te ramy wykracza, aczkolwiek nie można odmówić jej miana politycznej partycypacji. W tym kontekście internet jest narzędziem nie wyróżniającym żadnej ideologii, grupy politycznej czy instytucji. Jak było powyżej zaznaczone, wykorzystanie sieci stwarza nowe możliwości w różnych sferach politycznej aktywności (Porębski, 2001), w tym daje nowe narzędzia dla wyrażania obywatelskiego nieposłuszeństwa. Coraz częściej mamy bowiem do czynienia z różnorodnymi aktami protestu wobec działań instytucji i organów władzy państwowej, dla których to aktów nośnikiem jest właśnie sieć. Szczególnie interesującym przykładem wykorzystania funkcjonalności nowych mediów dla prowadzenia działalności społeczno-politycznej jest hakywizm. Określenie to powstało z połączenia słów „haker” i „aktywista”.

O ile wyjaśnienie pojęcia „aktywista” nie rodzi szczególnych problemów definicyjnych, to już określenie „haker” będzie nastroczało więcej komplikacji. „Aktywista” to nikt inny, jak zagorzały, mocno zaangażowany członek organizacji, społeczności. Można go określić przy użyciu sformułowań: społecznik, ochotnik, ideowiec. Według słownika języka polskiego: aktywista to członek organizacji, mocno zaangażowany w jej działalność (<http://www.sjp.pl/aktywista>, 2010). Co się zaś tyczy drugiego z wyjaśnianych terminów, to w języku potocznym słowo haker stało się synonimem komputerowego włamywacza i przestępcy komputerowego, elektronicznego wandalę, który korzystając ze zdalnych środków dostępu, dokonuje włamań do systemów informatycznych dla zabawy bądź w innym celu (Erickson, 2008).

„Gazeta Prawna” (2012) w swej encyklopedii zamieszcza definicję w brzmieniu: „haker – osoba o bardzo dużych praktycznych umiejętnościach informatycznych, odznaczająca się znajomością wielu języków programowania, a także świetną znajomością systemów operacyjnych oraz bardzo dobrą orientacją w Internecie”. Hakerzy sami siebie określają przede wszystkim jako specjalistów, których włamanie do chronionych komputerów dokonywane są jedynie po to, by obnażyć słabości systemów bezpieczeństwa i poinformować o nich właścicieli sforsowanych zabezpieczeń. Podstawowym założeniem hakerów jest nie niszczyć, a nadrzędnym celem jest doskonalenie swojej wiedzy i pisanie jak najlepszych programów. Subkultura ta nabrała silnych znamion elitarności, wynikających na początku ze słabej dostępności do komputerów, a teraz – bardziej z odcięcia się od wszelkich form komercyjnej działalności. Granica między działaniem w słusznej sprawie a czystą ciekawością i chęcią zaznaczenia swojej wiedzy bywa tu bardzo płynna (du Vall, 2010). Kanonem hakerskiej etyki jest nieskrępowane prawo do informacji, nawet jeśli znajduje się ona w cudzym komputerze. Można zgodzić się ze twierdzeniem, że to hakerzy zbudowali Internet, gdyż bez nich i bez ich anarchistycznej ideologii nigdy to medium nie zostałoby tak szybko stworzone i rozpowszechnione na całym świecie. Jako wierni członkowie tej subkultury podkreślają, że zrobili to w imię odwiecznych ludzkich pragnień stworzenia wspólnoty ludzi, którzy zamiast ze sobą walczyć, wymieniają między sobą informacje, doświadczenia, upowszechniają za darmo wiedzę (Mediologia, 2012). Generalizując można uznać, że dozwolone jest wszystko to, co inni użytkownicy sieci akceptują, zakazane zaś to, na co nie ma powszechnej zgody internautów. Trzeba podkreślić, że współczesne hakerstwo ma wiele twarzy, a jedną z nich jest hakywizm.

Znając etymologię terminu „haktywizm” warto zastanowić się nad motywami działania „sieciowych aktywistów”. Z reguły pobudki te mają charakter społeczny bądź polityczny. 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. Ideę obywatelskiego nieposłuszeństwa można rozumieć, jako swego rodzaju kontestację, co oznacza kwestionowanie czegoś, poddawanie w wątpliwość, demonstrowanie, manifestowanie sprzeciwu, protestu. Kontestator to osoba, która nie przestrzega powszechnych wzorców zachowań, bądź celowo je odrzuca, kierując się własnymi standardami, zgodnymi z wyznawaną hierarchią wartości (Majorek, 2007). Można przyjąć za Hannah Arendt, iż nieposłuszeństwo obywatelskie pojawia się wówczas, gdy znacząca liczba obywateli dochodzi do przekonania, że normalne kanały dokonywania zmian nie funkcjonują, a skargi nie zostaną wysłuchane lub uwzględnione, albo przeciwnie, że rząd chce dokonać zmian nie uwzględniając głosu obywateli (Arendt, 1999). W sytuacji, gdy obywatele traktowani są jak bezwolne automaty, społeczeństwo ma prawo odczuwać zbyt duże ograniczenie swojej wolności i protestować, łamiąc świadomie obowiązujące normy społeczne i prawne (du Vall, 2012). Zwolennicy aktywności mieszczącej się w zakresie obywatelskiego nieposłuszeństwa, podkreślają świadomy charakter takiej akcji, brak przemocy, a w szczególności zorientowanie na zainicjowanie określonych reform. Odrzucają oni zarzut, jakoby było to jedynie formą niedemokratycznej, politycznej taktyki, blisko związanej z innymi typami oporu wspartego na przemocy. Nie sposób jednak w prosty i zarazem zdecydowany sposób zaakceptować któregośkolwiek z tych sądów, a zatem warto poświęcić trochę miejsca refleksji w tym przedmiocie.

Zarzuty, jakie kierowane są pod adresem prób usprawiedliwiania wskazanych działań zawierają się zazwyczaj w następujących obiekcjach. W pierwszym rzędzie oczywistą kwestią jest nielegalność takich aktów, zatem kłóci się to z ideą zobowiązania do przestrzegania prawa danej państwowości, posiadanego przez obywateli demokratycznych wspólnot państwowych (Majorek, 2010, s.225). Ustrój demokratyczny zapewnia sprawowanie rządów zgodnie z literą obowiązującego prawa oraz dostęp do demokratycznych procedur, co umacnia w przekonaniu, iż obywatel ma obowiązek przestrzegać istniejących norm. *Możemy poszukiwać sposobów zmiany obowiązującego prawa, lecz nigdy poprzez jego nieprzestrzeganie* (Stettner, 1971, s.113) wskazywać będą teoretycy prawa zajmujący się tym problemem. Niewątpliwie jest to znacząca przesłanka, aczkolwiek nie można z asercją zaprzeczyć, iż wiele demokratycznych procedur, pomimo, iż są powołane do życia, nie funkcjonują prawidłowo, co może powodować częściowe lub całkowite wykluczenie pewnych, zwłaszcza mniejszościowych grup. W świetle powyższego, usprawiedliwienie obywatelskiego nieposłuszeństwa, musiałoby polegać na wykazaniu, iż tak rozumiane zobowiązanie do przestrzegania istniejących przepisów może zostać przeważone. Po drugie, jeśli system demokratyczny gwarantuje szereg legalnych środków, jakie mogą zostać zastosowane w działaniu politycznym, zapewne nieposłuszeństwo obywatelskie do takich się nie zalicza, zatem nie jest ono usprawiedliwione (Rostow, 1971). Jednakże można dalej utrzymywać, że każdy obywatel zamieszkujący demokratycznie zorganizowaną wspólnotę państwową, ma prawo (lub nawet zobowiązanie) występować przeciwko konkretnym przepisom, jakie w sposób jaskrawy naruszają istotne wolności lub też, ogólnie rzecz ujmując, tym, które naruszają szeroko pojmowane prawa człowieka. Z drugiej zaś strony, za nieuprawnione może być uznane działanie o znamionach nieposłuszeństwa, zastosowane w celach taktycznych, mające za zadanie doprowadzić do zmiany przepisów prawa, bądź aktualnej polityki demokratycznych władz. I w tym miejscu widać podstawowy problem współczesnych aktów politycznej partycypacji noszących znamiona nieposłuszeństwa, albowiem ci którzy ich dokonują, będą dążyć do klasyfikowania swych działań do tej pierwszej grupy, wskazując na naruszanie przez władze

podstawowych praw i wolności. W ten właśnie sposób prezentować będą swoje stanowisko hakywiści, podkreślając, iż przedsięwzięte przez nich działania przybierają formę pozbawionego przemocy protestu przeciwko instytucjom lub osobom podejmującym nieetyczne lub bezprawne czynności. Elektroniczne obywatelskie nieposłuszeństwo ma na celu informowanie w służbie ludzi, a nie instytucji (du Vall, 2010).

W aktach nieposłuszeństwa obywatelskiego bardzo istotną rolę odgrywa przepływ informacji. Jednostki porozumiewają się ze sobą w taki sposób, aby nie być już więcej oddzielnymi ludźmi, ale widoczną siłą. Udowadniają tym samym, że nawet mniejszości, jeżeli stowarzyszą się w grupy i stają się liczniejsze, to potrafią osłabić moralne panowanie większości. Elektroniczna przestrzeń przepływów, jaką stanowi internet, postrzegana jest obecnie przez aktywistów nie tylko, jako płaszczyzna komunikacji i informacji (sprawnego przekazywania treści i łatwego do nich dostępu), ale przede wszystkim jako narzędzie ekspresji swojego niezadowolenia i swoich przekonań; jako medium wywierające wpływ na świadomość społeczną z jednej strony, a z drugiej na politykę rządu. W związku z powyższym należy uznać, że po pierwsze internet jako wspomnianą wcześniej „autostrada informacyjna” stanowi swego rodzaju lustro, w którego odbiciu odnajdujemy współczesne społeczeństwo wraz z jego potrzebami, patologiami i słabościami. Po drugie zaś i dla autorek istotniejsze, narzędzie to wzmacnia polityczną skuteczność, podnosi poziom świadomości społeczno-politycznej, pobudza do aktywności publicznej i daje obywatelom poczucie sprawowania kontroli nad poczynaniami elit politycznych (Wojniak, 2010b).

### **Sieciowi aktywiści w działaniu – wybrane przykłady**

Protesty w krajach arabskich stanowią przykład „rewolucji 2.0”. Na nowo zdefiniowały one funkcje internetowych portali społecznościowych, takich jak Facebook i Twitter. Aktywność na platformach społecznościowych była czynnikiem istotnie ułatwiającym wymianę spostrzeżeń, dyskusję – a to popchnęło ludzi do przejścia z virtualu do „akcji bezpośredniej” na ulicach miast. Serwisy społecznościowe stały się podstawową siłą sprawczą wystąpień protestacyjnych, a młodzi internauci byli nośnikami procesów demokratyzacji w tym regionie, począwszy od wybuchu w grudniu 2010 roku rewolucji w Tunezji i upadku rządów prezydenta Zine Abidine Ben Alego, poprzez egipską Rewolucję 25 stycznia 2011 roku, skończywszy na rewolucji libijskiej oraz protestach w Egipcie, Jemenie, Jordanii i Syrii. Grupy i profile tworzone na Facebooku zachęcały obywateli do uczestnictwa w zgromadzeniach o charakterze pokojowego protestu (du Vall, Walecka-Rynduch, 2012).

Co istotne, w szybkim tempie nastąpił proces internacjonalizacji protestów. Dzięki nowoczesnym technologiom przekazu, informacja swobodnie rozprzestrzeniła się ponad granicami państw. Aktywiści z Niemiec, Szwecji, Holandii i Francji „linkowali” strony prowadzone przez bliskowschodnich dysydentów i krytycznych bloggerów, a szczególnie istotną rolę odegrała tu szybkość przekazywania informacji i jej zawartość polityczno-ideologiczna. Wyraźnie można w tym zjawisku dostrzec ogromną siłę oddziaływania nowych mediów na świadomość społeczną.

Innym przykładem działalności społeczno-politycznej wykorzystującej możliwości nowych mediów są akcje organizowane pod szyldem Ruchu Oburzonych. Ich sposób organizacji i metody działania od momentu powstania charakteryzuje pozioma, maksymalnie demokratyczna struktura. Ogromną rolę odgrywa komunikacja za pomocą stron internetowych, portali społecznościowych, list mailingowych. Ułatwia to budowanie struktury i dotarcie do ideowych sojuszników. Są to, jak widać, doskonałe narzędzia stosowane do mobilizacji zasobów społecznych. Posiłkując się teorią ruchów społecznych należy podkreślić, że komunikacja jest istotną częścią działania ruchu na każdym etapie jego rozwoju – jego powstania, utrzymywania się i w końcu legitymizacji. Dodatkowo to ona wyznacza też sukces lub porażkę ruchu w takich sferach jak: wpływanie na politykę państwa, zakresanie dyskursu publicznego,

wytwarzanie nowych identyfikacji kulturowych i wewnętrznej demokratyzacji. Ruchy społeczne bez wątpienia są tym obszarem, gdzie rodzą się nowe formy komunikowania i nowe perspektywy jego rozumienia (du Vall, Walecka-Rynduch, 2012).

Wyżej wspomniane zjawiska można określić hakytywizmem, jeśli przyjmiemy jego definicję sensu largo. Jednak dużo więcej problemów interpretacyjnych powodują działania sieciowych aktywistów stricte związane z działalnością hakerską (hakytywizm rozumiany wąsko). Przykładem organizacji, która na szeroką skalę korzysta z hackingu jest Grupa Anonymous, której członków łączy wspólny cel i wspólna idea. Przynależność do niej jest dobrowolna, oparta na zasadach horyzontalnej demokracji. Organizacja łączy ludzi, którzy podążają w tym samym kierunku i w każdej chwili można do niej dołączyć lub zdecydować się ją opuścić. Jeżeli jednostka chce być Anonimowym to staje się nim bez jakichkolwiek ograniczeń. Struktura przywództwa tej grupy stanowi także ciekawy element, bowiem Anonimowi nie mają przywódców, a zatem nie można nimi rządzić, można im jedynie proponować, sugerować pewne rozwiązania, bądź też kierunki dalszej aktywności. Nie są „niebezpiecznymi hakerami”, jak określają ich media, lecz są po prostu ludźmi, którzy swą ideologię czerpią wprost z anarchistycznego hackingu. Dbają by respektowane było prawo do szeroko pojmowanej wolności, walczą z cenzurą w internecie, inwigilacją, sprzedawaniem wiadomości i danych osobowych, z totalitaryzmem, z Kościołem Scjentologicznym (<http://www.anon.ssl2.pl/>, 2012). Nieco upraszczając, można napisać, iż w zasadzie Anonymous występują przeciwko organizacjom, które nie traktują swoich klientów zgodnie z przyjętymi normami etycznymi, ograniczają wolność poglądów, cenzurują albo niechlujnie traktują poufne dane (Łabuda, Pursche, 2012). Dla osiągnięcia swoich celów obrali pokojowe manifestowanie swojego protestu, głównie poprzez akcje informacyjne, uświadamiające ludziom kim są, z czym i o co walczą (<http://www.anon.ssl2.pl/>, 2012). Charakter organizacji i jej sposoby działania doskonale oddają słowa: „Jesteśmy legionem. Nie zapominamy. Nie wybaczymy. Spodziewajcie się nas” czy: „Nie schowacie się. Jesteśmy wszędzie”.<sup>3</sup> Kiedy te groźnie brzmiące hasła pojawiają się na serwerach rozmaitych firm i instytucji państwowych, mało zaskakującym wydaje się fakt, iż budzą one uzasadniony niepokój.



Źródło: materiały Anonimowi Polska, operacja Paperstorm  
<http://s1179.photobucket.com/albums/x381/gr0w33r/>

Anonimowi, jak czytamy na stronie internetowej, pokonali długą drogę. Kilka lat temu stanowili zaledwie niewielką grupę forumowiczów bez konkretnych planów na przyszłość. Dziś ich społeczność liczy ponad milion członków i zdolna jest unieruchomić duże portale, pozyskać z nich poufne dane, i co

<sup>3</sup> Słowa padają w słynnym filmie dot. Kościoła Scjentologicznego, autorstwa Anonymous, do obejrzenia pod adresem: <http://www.youtube.com/watch?v=JCbkv9yiLiQ> [marzec 2012]

szczególnie ważne, zgromadzić się poza wirtualną przestrzenią, by protestować na ulicach miast (<http://www.anonyops.ssl2.pl/>, 2012). Rzecz, która zasługuje na podkreślenie to fakt, iż komunikacja i przepływ informacji (wykorzystujący nowe media) działa w tej organizacji bezbłędnie. Organizacja Anonymous produkuje filmy oraz gromadzi, łączy i rozpowszechnia informacje. W polu jej zainteresowania znajdują się zwłaszcza te, które władze i firmy chcą wyeliminować z internetu za pomocą cenzury (Łabuda, Pursche, 2012). Dodatkowo, to co czyni ten ruch wyjątkowym, to to, że informacja o każdej „akcji” prędzej czy później trafia na strony główne internetowych serwisów, często również do telewizji i prasy. Masowe media stają się tym samym sojusznikiem Anonimowych w uświadamianiu przeciętnych obywateli, pomagają poznać przyczyny ataku, pozwalają wyrazić czytelnikowi opinie (fora, komentarze) i w dalszej kolejności (ewentualnie) zmienić stosunek do organizacji i przysporzyć jej nowych członków (<http://www.anonyops.ssl2.pl/>, 2012).

Działalność Anonimowych rozpatrywana jest w kontekście hakywizmu, gdyż wyraźnie widoczne są w nich polityczne lub społeczne pobudki „wkurzonych” internautów, którzy dzięki prostym wskazówkom i sile masy mogą rozłożyć infrastrukturę nawet największej firmy. Od 2010 r. roku hakerską działalność grup cyberaktywistów wiązano, między innymi, z poważnymi atakami na witryny Visa, MasterCard i PayPal (ich celem było ukaranie firm za to, że przestały przekazywać datki wpłacane na rzecz portalu Wikileaks). W dalszej kolejności przedmiotem działań stały się takie firmy i instytucje jak: NASA, Nintendo, Sony (pierwszy z ataków uderzył w Playstation Store, drugi w SonyPictures.com – ośmieszył on korporację, gdyż ujawnił, że wszystkie dane użytkowników były przechowywane w zwykłym, niezakodowanym w żaden sposób, tekście), Międzynarodowy Fundusz Walutowy. Nie dziwi zatem, że za cele obrano sobie również rządy wielu krajów, a nawet CIA. Większość ze wskazanych ataków odbyła się nie dzięki pojedynczym jednostkom, ale przy pomocy rozproszonych po całym świecie anonimowych internautów, którzy dobrowolnie przyłączali się do organizowanych na masową skalę ataków.

Aktywiści wykorzystują do swych ataków m.in. program o nazwie L.O.I.C (ang. Low Orbit Ion Cannon), czyli po polsku „niskoorbitowe działo jonowe”. Jest to żartobliwe nawiązanie do nazwy broni używanej w kultowej grze Command&Conquer z lat 90. Jednoczesne użycie programu przez tysiące połączonych przez Internet komputerów łączy ich moc obliczeniową i przeciąża serwery atakowanych stron zbędnymi danymi, aż do ich zawieszenia. Po skutecznym ataku hakywiści zawieszają na serwerze własne informacje, najczęściej biorą na siebie odpowiedzialność za przeprowadzoną akcję (Łabuda, Pursche, 2012). Anonimowi do arsenału swych wirtualnych narzędzi włączyli także rozproszony atak przeciążeniowy (ang. Distributed Denial of Service, w skrócie DDoS). Aplikacja ta tak długo „bombarduje” stronę aż ta przestanie reagować. Ten, można stwierdzić, systemowy atak obejmuje przekierowywanie użytkowników do specjalnie skonstruowanych stron internetowych, które wykorzystują JavaScript, aby „odesłać” odwiedzających do dowolnej witryny, która jest celem ataku. Program wielokrotnie próbuje uzyskać dostęp do atakowanej witryny, aż do jej całkowitego zawieszenia. Dla atakujących jest to bezpieczniejsza metoda, ponieważ widoczne są tylko adresy IP przypadkowych użytkowników. Z pomocą tego narzędzia została zaatakowana strona Universal Music, a do jej zablokowania wykorzystano wszystkich odwiedzających witrynę CBS.com (Jabłoński, 2012a).

Spektakularne ataki hakywistów miały miejsce od końca 2011 roku, a jedną z ich ofiar stał się Stratfor (Strategic Forecasting), ceniony dostawca analiz z zakresu obronności i geopolityki, wykorzystywanych przez armię USA, a nawet Białą Dom. Sieciowi aktywiści uzyskali nieautoryzowany dostęp do informacji o kontaktach subskrybentów ośrodka analitycznego. Baza danych zawierała dane 850 tys. osób korzystających z zasobów Stratford – zazwyczaj były to adresy e-mail oraz zaszyfrowane hasła, zapisane w arkuszach kalkulacyjnych. Po ataku hakerzy ujawnili numery kart kredytowych 75 tys.

abonentów, którzy płacą za dostęp do treści publikowanych na stronie Stratfor, w tym dane 462 użytkowników z Wielkiej Brytanii m.in. z Ministerstwa Obrony, Ministerstwa Spraw Zagranicznych, Scotland Yardu, Joint Intelligence Organisation (odpowiedzialnej za wsparcie wywiadu, w tym tajnych agentów słynnego MI6) i parlamentarzystów (<http://www.tvn24.pl/1,1730730,druk.html>, 2012). Hakerzy, którzy poinformowali o włamaniu do Stratfora, mieli maski Guya Fawkesa (cybernetyczny Robin Hood lub Janosik), zapowiedzieli, że środki z kart kredytowych klientów Stratfora zasila organizacje charytatywne.



Maska Guya Fawkesa z komiksu „V jak vendetta” stała się znakiem rozpoznawczym Anonimowych  
fot.za: <http://wiadomosci.onet.pl/cnn/ta-mask-a-stala-sie-symbolem-walki-z-chciwoscia,1,4899266,wiadomosc.html>

Na początku lutego 2012 r. świat obiegła wiadomość o kolejnej akcji Anonimowych. Tym razem atak dotknął amerykańskie Federalne Biuro Śledcze i brytyjski Scotland Yard. Aktywiści opublikowali na YouTube nagranie z poufnej telekonferencji, dotyczącej zwalczania przestępczości w cyberprzestrzeni, pomiędzy wyżej wymienionymi służbami<sup>4</sup>. Wraz z nagraniem konferencji, Anonimowi udostępnili też przechwyconego e-maila wysłanego przez agenta FBI, w którego treści widniały szczegółowe informacje na temat planowanej rozmowy, w tym hasła umożliwiające w niej udział. Konferencja odbyła się 20 stycznia 2012 roku, trwała 15 minut i głównie skupiała się na sposobach koordynacji walki z Anonymous i kilkoma innymi grupami hakerskimi. Agenci wymieniali się informacjami o planowanych aresztowaniach oraz działaniach wymierzonych w ważnych aktywistów ruchu (Jabłoński, 2012b).

Kolejnym przedsięwzięciem zakrojonym na szeroką skalę był atak Anonimowych na serwisy związane z ochroną praw autorskich, doprowadzający do ich unieruchomienia. Ofiarami ataku były strony: Amerykańskiego Departamentu Sprawiedliwości, Universal Music Group oraz organizacji RIAA i Motion Picture Association of America. Był to swego rodzaju odwet haktivistów za zamknięcie serwisu Megaupload<sup>5</sup>. Strona Megaupload należała do głównych serwisów internetowych zajmujących się wymianą plików. Została ona na początku roku 2012 zamknięta przez amerykańskie władze, a właściciele strony zostali aresztowani. Serwis miał ponad 50 milionów odwiedzin dziennie i 150 milionów użytkowników. Oczywiście nie była to działalność charytatywna – twórcy Megauploadu opracowali rozbudowany system ściągania opłat od użytkowników, jednocześnie wynagradzając tych najaktywniejszych. W Internecie można spotkać wiele podobnych serwisów, gdzie przechowywane są tylko pliki, które można później pobrać w prosty sposób. Nie brzmi to może szczególnie groźnie aż do momentu, gdy przyjrzymy się temu bliżej. Istotnie w ogromnej przewadze są to rozmaite pliki z filmami, muzyką czy programami, udostępniane niezgodnie z prawem (Jabłoński, 2012c). Nie zmienia to jednak

<sup>4</sup> Do wysłuchania pod adresem: [http://www.youtube.com/watch?feature=player\\_embedded&v=pl3spwzUZfQ](http://www.youtube.com/watch?feature=player_embedded&v=pl3spwzUZfQ) [marzec 2012]

<sup>5</sup> Megaupload to niemal synonim piractwa, choć oczywiście wielu użytkowników wykorzystuje go do legalnych celów. Jego polskim, mniejszym odpowiednikiem może być serwis Chomikuj.pl

faktu, że podobnie jak przy całym medialnym szumie i społecznym zamieszaniu ws. ACTA<sup>6</sup>, hakywiści w myśl swej wolnościowej ideologii walczą z systemem, który chce mieć władzę nad dostępem do informacji, wiedzy, kultury.

Jeśli chodzi o polski internet, to styczeń 2012 roku był miesiącem, w którym w tym medium zanotowano szczególne poruszenie. Sprawa ACTA wywołała ogromne oburzenie, szereg dyskusji, a przy okazji serię ataków na strony internetowe administracji państwowej RP.



Źródło: <http://www.polskieradio.pl/5/3/Artykul/521918,Atak-na-strony-rzadowe-w-odwecie-za-ACTA> [marzec 2012]

Celem Anonimowych stały się głównie strony w rządowej domenie gov.pl: Agencji Bezpieczeństwa Wewnętrznego, Ministerstwa Obrony Narodowej, Ministerstwa Gospodarki, Sejmu oraz Ministerstwa Sprawiedliwości. Rządowy Zespół Reagowania na Incydenty Komputerowe przygotował interesującą analizę, podsumowującą działania Anonimowych w dniach 21-25 stycznia 2012 roku. Dowiadujemy się z niej, że *przede wszystkim zaobserwowano ataki typu odmowa usług DDoS skierowane przeciwko serwerom WWW na których utrzymywane był strony ważniejszych instytucji administracji rządowej. Ataki miały na celu wysycenie łącza internetowego a przez to spowodowanie niedostępności strony WWW*. W szczytowych momentach serwisy rządu notowały około 23,000 odwiedzin na minutę (Kamiński, 2012). Można uznać, że dzięki ogromnej popularyzacji tematu ACTA w mediach, skala działań Anonimowych nie dała rządowym serwerom żadnych szans.

Wśród polskich przedsięwzięć Anonimowych warto również przywołać operację MailStorm z 2011 r., która polegała na przywróceniu wartości słów „wolność słowa” i przeciwstawieniu się bezprawnym zakazom wypowiedzianym, głównie chodziło o ks. Adama Bonieckiego. W ramach tego przedsięwzięcia skrzynki e-mailowe Zakonu Księży Marianów zostały zbombardowane ogromną ilością maili, których celem było zwrócenie uwagi na sytuację ks. Bonieckiego (<http://www.anonyops.ssl2.pl/operacje.html>, 2012).

Wśród innych polskich przykładów działalności hakywistów, nie koniecznie spod znaku Anonimowych, można wymienić, między innymi, głośną sprawę z końca 2010 roku. Cyberaktywista zaatakował strony internetowe Rady ds. Uchodźców oraz Państwowej Służby Hydrogeologicznej. Wcześniej ta sama osoba była odpowiedzialna także za włamanie na witrynę Centralnej Komisji Egzaminacyjnej. Wszystkie trzy wyżej wymienione strony zostały przez niego podmienione i sparaliżowane na kilka godzin. Mimo grożących za ten czyn sankcji „sprawca” nie został ukarany z

<sup>6</sup> ACTA - Anti-Counterfeiting Trade Agreement, to umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi. W umowie chodzi o walkę z naruszeniami własności intelektualnej. Najwięcej kontrowersji w ACTA wzbudza zapis dotyczący problemu rozpowszechniania dzieł prawnie chronionych przez Internet. Prace nad ACTA rozpoczęły się w 2005 roku. W 2011 roku porozumienie ws. ACTA przyjęły Rada Unii Europejskiej oraz polski rząd. Do przyjęcia ACTA przez Radę UE doszło podczas polskiej prezydencji w UE. Polska złożyła podpis pod ACTA 26 stycznia 2012 roku

prozaicznej przyczyny – braku skargi złożonej przez pokrzywdzonych (du Vall, 2012). Kolejnym zdarzeniem noszącym wyraźne znamiona protestu nowej ery, ery technologicznej był atak w pierwszy dzień roku szkolnego (1 września 2011) sieciowych aktywistów na kilkaset stron samorządowych<sup>7</sup> w naszym kraju. Na portalach, po kliknięciu na Biuletyn Informacji Publicznej, zamiast właściwych danych, pojawia się szkolny autobus (gimbus) i podpis zawierający m.in. stwierdzenie, że polskie szkoły uczą „spożywać duże dawki alkoholu”. Hakywiści podpisani *punkG* i *hardstyle77* napisali: *Polskie szkoły, zamiast kształcić młode społeczeństwo, robią z niego coś, co można nazwać zombie... W szkole nie nauczysz się odmian alotropowych, zjawiska hydrolizy i innych materiałów zawartych w podręcznikach. Dalej hakerzy dodają, że w polskich szkołach nauczysz się spożywać duże dawki alkoholu, palić trawkę oraz spożywać inne środki odurzające. Pomimo, że faktycznie strony www administracji rządowej i samorządowej znajdują się pod szczególną ochroną prawną<sup>8</sup>, to znikoma szkodliwość „występku” czyni go klasycznym przykładem wyrazu niezadowolenia, protestu wobec obowiązującego w naszym kraju systemu edukacji (du Vall, 2012).*

## **Podsumowanie**

Wnioski jakie wypływają z powyższych rozważań są w zasadzie jednoznaczne. W pierwszym rzędzie nasuwa się konstatacja, iż rozwój nowych mediów oraz współczesnych narzędzi komunikacji otwiera nieznane dotąd przestrzenie partycypacji społecznej, a także politycznej. Niewątpliwie za pozytywną cechę tej ekspansji uznać należy wzrost świadomości politycznej jednostek, co pociąga za sobą równoczesny przyrost ich aktywności w polu pozostającym dotychczas w zainteresowaniu jedynie niewielkiej mniejszości. Zwłaszcza wśród młodych ludzi obserwowano wcześniej apatię i brak zainteresowania bieżącymi sprawami, co za sprawą nowych narzędzi uczestnictwa w wydatny sposób się zmienia. Warto zaznaczyć, że zmiana ta dokonuje się właśnie w obecnej chwili, na naszych oczach bierność przeradza się w aktywność, przy niezaprzeczalnym udziale nowych technologii informacyjnych. Co więcej trend ten nie jest właściwy jedynie bogatym krajom tak zwanej starej Unii, czy też innym zamożnym demokracjom zachodnim. Jest on obecny także w krajach, w których dotychczas funkcjonowały demokracje fasadowe, a zamożność społeczeństwa również nie wskazywałaby na szeroką dostępność nowych technologii. Powyższe przykłady świadczą o tym, iż także na rodzimym gruncie nie brakuje aktów wymagających zarówno dostępu do nowoczesnych narzędzi komunikacji, posiadania wystarczającej wiedzy zakresu nowych technologii i prawa oraz świadomości politycznej podmiotów przeprowadzających opisane akty. Abstrahując od formy zaprezentowanej aktywności, za pozytywną cechę uznać należy sam fakt jej istnienia, co może zwiastować dramatyczny i zarazem nieustannie postępujący wzrost partycypacji politycznej polskiego społeczeństwa.

<sup>7</sup> Zaatakowane zostały strony samorządów lokalnych, m.in. powiatu żyrdowskiego, gmin: Włocławek, Jedlińsk, Ożarów, miast: Radzymin i Sulejówkę. Ofiarą hakerów padły także portale m.in.: Naczelnej Izby Pielęgniarek i Położnych, Radomskiej Stacji Pogotowia Ratunkowego, czy Gminnego Domu Kultury i Biblioteki w Głogowie Małopolskim, za: [http://www.gazetaprawna.pl/wiadomosci/artykuly/543645,wielki\\_atak\\_hakerow\\_na\\_portale\\_samorzadowe\\_kilkaset\\_stron\\_nie\\_dziala.html](http://www.gazetaprawna.pl/wiadomosci/artykuly/543645,wielki_atak_hakerow_na_portale_samorzadowe_kilkaset_stron_nie_dziala.html) [10.2011]

<sup>8</sup> W szczególności chronione są systemy informatyczne istotne dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, samorządowej lub innego organu państwowego. Taki sabotaż informatyczny oznacza niszczenie, uszkodzenie, usuwanie lub też wprowadzanie zmian dokonywane w stosunku do systemów dowodzenia, systemów istotnych dla kierowania i kontroli komunikacji kolejowej czy powietrznej, czy też innych istotnych systemów informatycznych organów administracji państwowej za: [http://prawo.gazetaprawna.pl/artykuly/451930,hakerzy\\_beda\\_scigani\\_z\\_urzedu.html](http://prawo.gazetaprawna.pl/artykuly/451930,hakerzy_beda_scigani_z_urzedu.html) [10.2011]

## Bibliografia:

- Arendt H. (1999), *O przemocy. Nieposłuszeństwo obywatelskie*, Warszawa.
- Cornwall A., Gaventa J., *Bridging the Gap: Citizenship, Participation and Accountability*, <http://www.iied.org/pubs/pdfs/G01927.pdf>.
- Erickson J. (2008), *Hacking: the art of exploitation*, San Francisco.
- Goban-Klas T., *W stronę społeczeństwa medialneg*, <http://www.ap.krakow.pl/ptn/ref2005/goban.pdf>.
- Jabłoński J. (2012a), *Anonymous atakuje za pomocą DDoS*, <http://magazynt3.pl/anonymous-atakuje-za-pomoca-ddos/>.
- Jabłoński J. (2012b), *FBI podsłuchiwane przez Anonimowych*, <http://magazynt3.pl/fbi-podsluchiwane-przez-anonimowych/>.
- Jabłoński J. (2012c), *Grupa hakerska Anonymous atakuje w odwecie za zamknięcie Megaupload*, <http://magazynt3.pl/grupa-hakerska-anonymous-atakuje-w-odwecie-za-zamkniecie-megaupload/>.
- Jaskiernia A. (2006), *Publiczne media elektroniczne w Europie*, Warszawa.
- Kamiński M. (2012), *Podsumowanie styczniowych ataków na strony rządowe. Premier chce odrzucenia ACTA!*, <http://antyweb.pl/podsumowanie-styczniowych-atakow-na-strony-rzadowe-premier-chce-odrzucenia-acta/>.
- de Kerckhove D., *Inteligencja otwarta. Narodziny społeczeństwa sieciowego*, Warszawa 2001.
- Kenski K., Stroud N. J. (2006), *Connections between Internet Use and Political Efficacy, Knowledge, and Participation*, "Journal of Broadcasting and Electronic Media", Vol. 50.
- Łabuda J., Pursche O. (2012), *Anonymous - dlaczego atakowali Sony, MasterCard i innych? Ekskluzywny wywiad*, za: <http://www.komputerswiat.pl/blogi/blog-redakcyjny/2011/06/nowe-zagrozenia,3.aspx#content>.
- Majorek M. (2007), *Pomiędzy społeczeństwem obywatelskim, a obywatelskim nieposłuszeństwem. Kontestacja społeczna jako forma współczesnej postawy obywatelskiej*, w: *Samotność idei? Społeczeństwo obywatelskie we współczesnym świecie*, red. B. Krauz-Mozer, T. Borowiec, Kraków.
- Majorek M. (2010), *Zobowiązanie: wolność czy zniewolenie? Moralny i polityczny wymiar zobowiązań*, „Episteme” 10/2010, t. I.
- Porębski L. (2001), *Elektroniczne oblicze polityki. Demokracja, państwo, instytucje polityczne w okresie rewolucji informacyjnej*, Kraków.
- Rostow E. V. (1971), *The Rightful Limits of Freedom in a Liberal Democratic State: of Civil Disobedience* [w:] Rostow E.V. (red.) *Is Law Dead?*, New York.
- Stettner E. A. (1971), *Political Obligation and Civil Disobedience*, „Polity”, vol. 4, nr 1.
- du Vall M. (2010), *Electronic Civil Disobedience (ECD) jako jedna ze współczesnych form obywatelskiego nieposłuszeństwa*, w: „Państwo i Społeczeństwo” red. S. Kilian, nr 1/2010.
- du Vall M. (2012), *Nieposłuszeństwo obywatelskie w XXI wieku*, w: *Dylematy polskiej demokracji*, red. Ł. Danel, J. Kornaś, Kraków.
- du Vall M., Walecka-Rynduch A. (2012), *Wyzwania komunikacyjne wobec polityki protestu*, w: *Public relations wobec wyzwań współczesności*, red. G. Piechota, Kraków.
- Wojniak J. (2010a), *Uczestnictwo polityczne w obliczu nowych technologii informacyjnych i komunikacyjnych*, w: „Stare” i „nowe” media w kontekście kampanii politycznych i sprawowania władzy, red. M. du Vall, A. Walecka-Rynduch, Kraków.
- Wojniak J. (2010b), *Globalne społeczeństwo sieciowe jako ponowoczesna przestrzeń socjotechniki politycznej*, Kraków (niepublikowana praca doktorska).
- <http://www.sjp.pl/aktywista> (21 marca 2012).
- Gazeta Prawna (2012), <http://www.gazetaprawna.pl/encyklopedia/prawo/hasla/332774,haker.html>, 2012, (8 Marca 2012).
- Mediologia.pl, 2012, <http://mediologia.salon24.pl/383917,hakerzy-prawdziwi-wlasciciele-internetu>, (20 marca 2012).
- <http://stosunki.pl/?q=content/od-%C5%BAr%C3%B3d%C5%82-rozrywki-do-motoru-przemian-portale-spo%C5%82eczno%C5%9Bciowe-na-bliskim-wschodzie> (22 marca 2012).
- <http://www.anon.ssl2.pl/> (20 marca 2012).
- <http://www.anonyops.ssl2.pl/> (20 marca 2012).
- <http://www.youtube.com/watch?v=JCbKv9yiLiQ> (20 marca 2012).
- <http://s1179.photobucket.com/albums/x381/gr0w33r/> (8 marca 2012).
- <http://www.tvn24.pl/1,1730730,druk.html> (21 marca 2012).
- [http://www.youtube.com/watch?feature=player\\_embedded&v=pl3spwzUZfQ](http://www.youtube.com/watch?feature=player_embedded&v=pl3spwzUZfQ) (21 marca 2012).
- <http://wiadomosci.onet.pl/cnn/ta-mask-a-stala-sie-symbolem-walki-z-chciwoscia,1,4899266,wiadomosc.html> (10 stycznia 2012).
- <http://www.polskieradio.pl/5/3/Artykul/521918,Atak-na-strony-rzadowe-w-odwecie-za-ACTA> (21 marca 2012).
- [www.cert.gov.pl](http://www.cert.gov.pl) (20 marca 2012).
- [http://prawo.gazetaprawna.pl/artykuly/451930,hakerzy\\_beda\\_scigani\\_z\\_urzedu.html](http://prawo.gazetaprawna.pl/artykuly/451930,hakerzy_beda_scigani_z_urzedu.html) (8 marca 2012).
- [http://www.gazetaprawna.pl/wiadomosci/artykuly/543645,wielki\\_atak\\_hakerow\\_na\\_portale\\_samorzadowe\\_kilkaset\\_st\\_\ron\\_nie\\_dziala.html](http://www.gazetaprawna.pl/wiadomosci/artykuly/543645,wielki_atak_hakerow_na_portale_samorzadowe_kilkaset_st_\ron_nie_dziala.html) (8 marca 2012).