DOI: 10.14746/r.2018.1.4

Faustyna KOWALSKA

Uniwersytet im. Adama Mickiewicza w Poznaniu

Hakerzy w służbie państwa – wirtualna strona patriotyzmu

Streszczenie: Współcześnie cyberprzestrzeń jest przestrzenią alternatywną do świata fizycznego. Każde zachowanie człowieka może znaleźć odzwierciedlenie w świecie wirtualnym, tak jak dzieje się od kilkudziesięciu lat w przypadku zjawisk negatywnych: przestępstw czy szeroko rozumianych walk. Społeczeństwo sieciowe szczególną wagę przykłada do obrotu informacją, która w obliczu natłoku wiedzy bezużytecznej stanowi cenne dobro. Ten kto posiada informacje i potrafi je w odpowiedni sposób wykorzystać, sprawuje władzę. W artykule poruszono wpływ pracy i zaangażowania hakerów na rzecz bezpieczeństwa państwa oraz motywacje ich zachowania.

Słowa kluczowe: haker, cyberbezoieczeństwo, patriotyzm

Niespełna dwadzieścia lat temu telefony z czarno-białym wyświetlaczem, komputery z ekranem kineskopowym i przewodowy Internet były w Polsce nadzwyczajnymi wynalazkami. Od tego czasu świat zmienił się na tyle, że ludzie zapomnieli o nich na rzecz nowoczesnych smartfonów, laptopów oraz coraz bardziej powszechnego ibezpłatnego dostępu do sieci WiFi. Nie sposób wymienić wszystkich nowinek technologicznych, które powstają każdego dnia i wciąż są ulepszane przez międzynarodowe korporacje i mniejsze firmy. Liczba użytkowników, korzystających z sieci wzrasta oraz rozpowszechnia połączenia sieciowe w różnych dziedzinach aktywności społecznej (Madej, 2009, s. 21–22), dając początek społeczeństwu informacyjnemu. Elektronika, telekomunikacja, informatyka w ciągu ostatnich kilkudziesięciu lat zanotowały niezwykły postęp technologiczny. Rozwój w tych dziedzinach miał ogromny wpływ na współczesne społeczeństwo w każdej sferze życia począwszy od procesów społeczno-gospodarczych po kulturowe, na konfliktach zbrojnych kończąc.

Zdaniem M. Castellsa, globalnie organizujące się społeczeństwo powiązanych sieciowo społeczności i organizacji lokalnych oraz regionalnych jako społeczeństwo ery informacji odznacza się łączeniem się

środowisk w niezliczone, złożone powiązania informacyjne. Istotną rolę odgrywa przy tym instytucjonalizacja i odtwarzanie sieci zbudowanej z węzłów, z możliwością przesyłania informacji, relacjami społecznymi i instytucjonalizującymi, a także dającymi możliwość przepływu władzy. Sieć ta wykorzystywana jest przez współpracujące ze sobą w sferze administracji i zarządzania podmioty (Castells, 2010, s. 465–468).

Definicje systemów teleinformatycznych i cyberprzestrzeni

Dzięki rewolucji technologicznej i gwałtownym przemianom procesu globalizacji, ludzie mają możliwość powszechnego i szybkiego dostępu do zasobów informacyjnych. Od informacji, jej zdobycia lub podjęcia, a nawet świadomości jej istnienia, zaczyna się wszelkie działanie. Informacja jest w dzisiejszym świecie jednym z podstawowych zasobów zarówno każdego państwa, organizacji, jak i poszczególnych osób. Współcześnie informacja, mając swoją wartość, stała się towarem i jest wyjątkowym dobrem niematerialnym. Dane państwo posiada swoje tajemnice w postaci informacji, które chroni, równocześnie chcąc poznać tajemnice innego państwa. Każde państwo też, mimo zawieranych układów i sojuszy, próbuje utrzymać w tajemnicy informacje, które miałyby wpływ na jego bezpieczeństwo. Każdego dnia informacje narażone są na nowe zagrożenia, głównie za sprawą komputerów i dostępu do Internetu (Reguła, 2015). Na Internet składają się: zespół komputerów i urządzeń peryferyjnych powiązanych liniami transmisji danych. Może skupiać nieokreśloną liczbę komputerów zintegrowanych za pośrednictwem modemów, łączy satelitarnych, światłowodów, linii radiowych na całym świecie, dzięki czemu umożliwia użytkownikom błyskawiczną komunikację bez ograniczeń terytorialnych niepodlegającym jurysdykcji poszczególnych państw (Hofmokl, 2009, s. 60–63).

System teleinformatyczny w rozumieniu polskiego ustawodawcy można zdefiniować jako zespół skorelowanych ze sobą urządzeń informatycznych oraz oprogramowania. Zapewnia on przetwarzanie, przechowywanie, wysyłanie i odbieranie danych za pomocą sieci telekomunikacyjnych i właściwego telekomunikacyjnego urządzenia końcowego (czyli urządzenia przeznaczonego do bezpośredniego lub pośredniego podłączenia do zakończeń sieci) (Ustawa z 18 lipca 2002 r., s. 2; Ustawa z 16 lipca 2004 r., s. 7). Bezpieczeństwo teleinformatyczne jest szczególnie istotne dla polityki państwa, ponieważ dotyczy wszystkich jej sektorów. Poza bezpieczeństwem militarnym czy społeczno-ekonomicznym, teleinformatyka ma

znaczenie przede wszystkim ze względu na ochronę danych osobowych, zagrożenie patologiami, czy rozwój gospodarczy. W ustawie o zarządzaniu kryzysowym z 2007 roku można przeczytać zapis włączający systemy teleinformatyczne do infrastruktury krytycznej, za którą uważa się systemy oraz wchodzące w ich skład funkcjonalnie ze sobą powiązane obiekty kluczowe dla bezpieczeństwa i obywateli, służące zapewnieniu efektywnego funkcjonowania organów administracji publicznej oraz instytucji i przedsiębiorców (Ustawa z 26 kwietnia 2007 r., s. 1). Objęte przez infrastrukturę krytyczną systemy opierają się na rozwiązaniach telekomunikacyjnych. Definicja teleinformatycznej infrastruktury krytycznej przedstawia ją jako systemy i sieci teleinformatyczne, których uszkodzenie lub nieodpowiednie funkcjonowanie (niezależnie z jakiego powodu i w jakim stopniu) może spowodować znaczące zagrożenie dla życia i zdrowia ludzi, bezpieczeństwa państwa i obywateli, interesów obronności lub narazić te interesy na szkodę (Krasnodębski, 2008, s. 1).

Możliwość przeniesienia znacznej części życia codziennego do świata wirtualnego spowodowała zwrot naukowców zajmujących się bezpieczeństwem w kierunku cybernetyki. Aby jak najlepiej zrozumieć czym dokładnie jest rzeczywistość oparta na technologii informatycznej, należy przeanalizować czym jest cyberprzestrzeń. Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 roku określa cyberprzestrzeń jako przestrzeń, w której zostają przetworzone i wymieniane informacje tworzone przez systemy teleinformatyczne, powiązania między nimi oraz relacje między ich użytkownikami (*Doktryna*..., 2015, s. 7).

Ochrona cyberprzestrzeni to jej niezakłócone działanie dzięki serii przedsięwzięć organizacyjno-prawnych, fizycznych, edukacyjnych i technicznych (*Rządowy Program*..., 2010, s. 6). Celem zabezpieczania jest przede wszystkim cyberbezpieczeństwo, czyli tok zapewniania bezpiecznego działania w cyberprzestrzeni: rozmaitych struktur, osób fizycznych oraz prawnych (w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej), będących w ich dyspozycji systemów teleinformatycznych i zasobów informacyjnych (*Doktryna*...., 2015, op. cit., s. 8).

Istota działania hakerów

W dzisiejszych czasach jednym z elementów ochrony cyberprzestrzeni jest odpowiedzialność społeczeństwa i jego zamierzone w tym zakresie działania. Zdarza się tak, że aktywiści działający w Internecie wykorzy-

stują narzędzia komunikacyjne i informacje jako kapitał we wzrost bezpieczeństwa zarówno indywidualnego, jak i zbiorowego. Przestrzeń wirtualna staje się naturalną przestrzenią aktywności członków społeczności lokalnych, państwowych i globalnych (Du Vall, 2014, s. 97).

Budowanie bezpieczeństwa cybernetycznego poprzez aktywną obronę, ulepszanie jej konkretnych faz, większą efektywność współpracy międzynarodowej, profesjonalizację sektora walki z przestępczością cybernetyczną oraz efektywną ochronę technologiczną staje się domeną grup hakerów na całym świecie. Jest to forma bezpieczeństwa, która powinna pozostawać w gestii państwa, co wynika z potrzeby zminimalizowania ryzyka popełnienia błędu w momencie legitymizacji podmiotu, który dopuszcza się interwencji. Współcześnie państwa skupiają się przede wszystkim na obronie pasywnej, czyli ulepszaniu zabezpieczeń elementów, które mogą być przedmiotem ataku. Wyprzedzenie terrorystów, aktywne ograniczenie form ich ataków oraz przygotowanie kontrataku, wykrywanie i udaremnianie popełnionych przestępstw są konieczne w świecie, w którym Internet odgrywa bardzo ważną rolę (Szulc-Wałecka, 2014, s. 288–290).

Pojęcie hakingu w społeczeństwie ma wydźwięk pejoratywny. Kojarzy się ono z cyberprzestępstwem: bezprawnym uzyskaniem dostępu do informacji znajdującej się w sieci, przełamywaniem elektronicznych bądź informatycznych zabezpieczeń. Niemniej jednak dla hakerów takie pojmowanie tego zjawiska jest niesprawiedliwe. W kulturze hakerskiej nadrzędnymi wartościami są wolność, technologie informatyczne i ich wykorzystywanie. Działania niezgodne z prawem noszą miano crackingu (Góra, 2015). Zawiłości terminologiczne pomiędzy hakerami i crackerami są przedmiotem sporów. Hakerzy nazywają przestępców związanych z technologiami informatycznymi crackerami, ci z kolei hakerów określają mianem włamywaczy sieciowych.

Według M. Castellsa, hakerzy nie są maniakami komputerowymi, którym zależy wyłącznie na łamaniu zabezpieczeń, zakłócaniu ruchu w sieci czy nielegalnej penetracji systemów. Hakerzy, to takie osoby, które za takie uchodzą w kulturze hakerskiej – wspólnocie złożonej z doświadczonych programistów i ekspertów w dziedzinie sieci komputerowych. Kultura ta sięga czasów pierwszych komputerów pracujących pod systemami operacyjnymi z podziałem czasu i pierwszych eksperymentów z ARPANetem (bezpośrednim przodkiem Internetu) (Castells, 2003, s. 52–53).

Kultura hakerów odnosi się głównie do zbioru norm i wartości, wykształconych w grupie programistów komputerowych, którzy współpra-

cują ze sobą za pośrednictwem sieci przy realizowaniu samodzielnie zdefiniowanych projektów, które związane są z twórczym wykorzystaniem komputerów. Duże znaczenie dla tej kultury odgrywa wolność rozumiana jako wolność tworzenia, korzystania z wszelkiej wiedzy i dzielenia się tą wiedzą w wybranej przez hakera formie (za pomocą dowolnych kanałów). Poczucie wolności stanowi ważny składnik ich światopoglądu oraz wpływa na ich sposób postępowania. Wolność w tym przypadku wiąże się z współpracą w ramach tak zwanej kultury daru (prowadzącej do ekonomii daru). Zarówno prestiż, reputacja, jak i szacunek, biorą się u hakerów ze znaczenia daru, jaki mogą przekazać społeczności. Haker może na przykład udostępnić swój program w sieci, niekoniecznie licząc na rewanż. Znaczenie ma przede wszystkim zademonstrowanie swojego talentu. Uznanie jest zdobywane nie tylko przez ofiarowanie społeczeństwu czegoś cennego, ale również przez to, że zrobiło się coś innego, odmiennego od innych. Dla hakerów radością jest sam akt tworzenia czy działania. Pieniądze, oficjalna własność intelektualna czy też pozycja zawodowa nie zapewniają hakerom autorytetu. Wynika on przede wszystkim z umiejętności technicznych (Ibidem, s. 57–59).

Istnieje klasyfikacja hakerów, która dzieli ich na trzy grupy:

1) *Black hat* (czarny kapelusz) – to tak zwani hakerzy, którzy łamią prawo bądź działają na jego granicy (ich dewiza brzmi, co nie jest zabronione, jest dozwolone), znajdując lukę w systemie wykorzystują ją do własnych, niekoniecznie legalnych celów;
2) *White hat* (biały kapelusz) – haker, którego cechuje unikanie sytuacji, w których może wyrządzić szkodę. Często takie osoby można spotkać, jako etatowych pracowników rozmaitych firm czy instytucji. Gdy *white hat* znajdzie lukę w systemie zabezpieczeń zgłasza ją osobie odpowiedzialnej za bezpieczeństwo danej jednostki (Michalik);
3) *Gray hat* (szary kapelusz) – działalność tej grupy hakerów nawiązuje do *black* i *white hats*. Jest to grupa osób, która zajmuje się z reguły legalnym testowaniem zabezpieczeń, jednakże zdarza im się przekroczyć granice legalności;
4) Cyberterrorysta – wykorzystuje cyberprzestrzeń, aby wyrządzić szkodę znacznej liczbie osób lub państwu. Aktywność cyberterrorystów skutkuje na przykład wyłączeniem sieci energetycznej w kraju, zaburzeniem centrum kontroli powietrznej i sprowadzeniem zagrożenia katastrofy lotniczej i tak dalej (Surgut, 2017).

Świat hakerów jest różnorodny, jednak całą grupę łączy wiara w potęgę sieci komputerowych oraz niezłomne postanowienie, aby były one

dobrem wspólnym nie tylko dla społeczności hakerskiej, ale ludzi na całym świecie.

Zagrożenia cyberprzestrzeni i sposoby działania hakerów w kontekście państwa

Bez względu na to jakimi pobudkami kierują się hakerzy, charakteryzują się oni biegłością w zagadnieniach technicznych. Wykształciła się u nich postawa szacunku do kompetencji. Mimo, iż są oni z reguły anonimowi inni użytkownicy Internetu doceniają ich za inteligencję, ciężką pracę i innowacyjne sposoby rozwiązywania problemów. Zainteresowania hakerów skupiają się przede wszystkim w takich obszarach jak:

1) systemy zabezpieczeń;
2) luki w systemach autoryzacji;
3) niedociągnięcia w programach (w tym operacyjnych);
4) przejmowanie nadzoru nad danym systemem;
5) metody elektronicznego kamuflażu;
6) tworzenie i działanie systemów operacyjnych;
7) znajomość zagadnień dotyczących agresji teleinformatycznej (Heuristic, 2017).

Każdego roku obserwuje się wzrost liczby zagrożeń spowodowanych przestępczością teleinformatyczną (z angielskiego *ICT Crime*). Przestępcy – *crackerzy* udoskonalają metody ataków oraz stawiają sobie coraz ambitniejsze cele. Do zagrożeń z uwagi na działania celowe oraz bezpieczeństwo państwa należą:

1) oprogramowanie złośliwe:
   – wirus – program destrukcyjny lub utrudniający korzystanie z komputera. Do rozprzestrzeniania potrzebuje nosiciela, innego programu komputerowego bądź dokumentu,
   – robak sieciowy – program, który samorozprzestrzenia się w sieci komputerowej. Nie potrzebuje nosiciela, żeby się rozprzestrzeniać,
   – koń trojański – złośliwe oprogramowanie o niepożądanej, utajonej funkcjonalności. Podszywa się pod aplikacje i służy wykradaniu haseł, czy śledzeniu pracy użytkownika,
   – dialer – program, który umożliwia łączenie się z siecią. Może być zainstalowany bez wiedzy i zgody użytkownika,
   – botnet (tak zwany komputer zombie) – podłączony do sieci komputer, na którym złośliwe oprogramowanie daje możliwość jego

zdalnej kontroli. Może być wykorzystywany do kradzieży danych użytkowników, na których są zainstalowane, czy do rozsyłania SPAMu;

2) przełamanie zabezpieczeń:
   – nieuprawnione logowanie,
   – włamanie na konto,
   – włamanie do aplikacji;
3) publikacje w Internecie – dezinformacja;
4) gromadzenie informacji:
   – skanowanie,
   – podsłuch,
   – inżynieria społeczna – na przykład *phishing* (wyłudzanie informacji, loginów, haseł przez podszywanie się pod instytucję lub zaufaną osobę. Stosowanie fałszywych stron internetowych, które wyglądają jak prawdziwe, ale wykradają dane poufne, na przykład do konta użytkownika):
      – szpiegostwo,
      – SPAM – niechciane wiadomości elektroniczne, najczęściej masowe. Z reguły rozsyłane do wielu odbiorców, niosą jednakową treść;
5) sabotaż komputerowy:
   – nieuprawniona zmiana informacji,
   – nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji,
   – atak odmowy dostępu (na przykład DDoS – atak, który uniemożliwia użytkownikowi prawidłowe działanie. Przeprowadzony z wielu komputerów w tym samym czasie, może polegać na atakowaniu serwera bardzo dużą ilością prób nawiązania połączeń,
   – skasowanie danych,
   – wykorzystanie podatności w urządzeniach,
   – wykorzystanie podatności aplikacji;
6) czynnik ludzki:
   – naruszenie procedur bezpieczeństwa,
   – naruszenie obowiązujących przepisów prawnych (Katalog zagrożeń CERT) (Gorzelak, Jacewicz, 2012, s. 2).

Liczba zagrożeń, które naruszają bezpieczeństwo systemów teleinformatycznym wzrasta. Na świecie wydaje się coraz więcej pieniędzy, aby zapewnić ochronę tych systemów. Niemal codziennie media podają informacje o udanych atakach cyberprzestępców na duże i małe firmy

i rządy państw (Jesiołek, 2013). Departament handlu USA szacuje straty amerykańskich firm na skutek cyberprzestępstw na 200–250 miliardów dolarów w roku 2014. Wykradane dane mogą służyć do manipulowania rynkiem i obrotami giełdowymi (Kaczmarek, 2014). Korzystając z Internetu, ludzie nie czują się już tak bezpiecznie jak kiedyś, przez co wzrasta poczucie niepewności. Mimo, że coraz więcej organizacji czy instytucji państwowych oferuje usługi elektroniczne, użytkownicy nie mają pewności czy ich dane są wystarczająco chronione, dlatego nie wykorzystują w pełni ich możliwości.

Współczesna, skuteczna administracja lokalna i państwowa jest zależna od efektywnego działania systemów teleinformatycznych. Umożliwiają one szereg przedsięwzięć: politycznych, ekonomicznych, militarnych, społecznych i tak dalej. Komputeryzacja systemów odpowiedzialnych za funkcjonowanie państwa (między innymi urzędów administracji publicznej, ochrony zdrowia, infrastruktury krytycznej, gospodarki) sprawiła, że stanęły one przed nowymi wyzwaniami w obszarze bezpieczeństwa. Cyberprzestrzeń stała się nowym polem walk i wojen między podmiotami państwowymi oraz pozapaństwowymi.

Podobnie jak w przypadku cyberprzestępstw, techniki walki informacyjnej i cyberwojny mogą być takie same. Opierają się na wszelkiego rodzaju wirusach, szpiegostwie, łamaniu zabezpieczeń, sabotażu, i tak dalej.

Coraz więcej państw tworzy formacje specjalnych grup operacyjnych hakerów, którzy mają za zadanie działanie w interesie danego państwa. Zdarza się również, że sami hakerzy organizują się, aby strzec bezpieczeństwa państw. Takie grupy specjalizują się między innymi we włamywaniu do rządowych baz danych innych państw bądź zabezpieczaniu systemów teleinformatycznych ojczyzny.

Kolejną grupą działającą na rzecz państwa w cyberprzestrzeni są tak zwani cyberżołnierze. Arena działań wojennych przeniosła się do cyberprzestrzeni już wiele lat temu. Obecnie wiele państw tworzy w szeregach swoich armii specjalne jednostki wyspecjalizowane do walki w cyberprzestrzeni. Internet jest kolejnym miejscem (po lądzie, wodzie, powietrzu i kosmosie), gdzie prowadzone są działania wojenne. Ich działania obejmują jednak znacznie większe terytorium niż Internet, na przykład sposoby przejmowania kontroli nad latającymi jednostkami, zakłócanie łączności radiowej i satelitarnej. Jednostki te mają zarówno bronić cyfrowych zasobów armii, jak i opracowywać scenariusze działań dotyczące neutralizacji elektronicznych systemów przeciwników (Surgut, 2017).

Hakerzy działający na rzecz państw

Trendem i ciekawym zjawiskiem w cyberprzestrzeni staje się analiza cyberataków przeprowadzanych na instytucjach państwowych przez administrację innych państw (na przykład Chiny zlecają hakerom wykradanie informacji bądź doprowadzanie do wycieku danych w zachodnich firmach i instytucjach, które są potem udostępniane spółkom kontrolowanym przez administrację państwową na terenie Chin, Rosji czy Korei Północnej). M. Hypponen uważa, że współcześnie od dłuższego czasu mamy do czynienia z sytuacją, w której toczy się walka pomiędzy siłami wojskowymi i cywilnymi o to, kto ma kontrolować rejestry, serwery, łącza oraz Internet. Prawdą jest, że każdy kraj posiada zarówno defensywne, jak i ofensywne zdolności w dziedzinie cyberbezpieczeństwa. Dużo wiadomo o możliwościach takich państw, jak Stany Zjednoczone, Rosja, Chiny, Wielka Brytania, które to maksymalnie starają się rozwijać swoje zdolności. Cyberbroń jest jednak niewidoczna, nie można więc odstraszyć przeciwnika samymi groźbami, ale dopiero kiedy faktycznie zostanie użyta, można przekonać się o jej możliwościach (Mikko).

W Polsce coraz częściej mówi się o utworzeniu cyber armii ochotników, której ideą byłoby włączenie środowisk hakerskich we wsparcie działań na rzecz obrony kraju. W wielu państwach na całym świecie istnieją osoby cywilne, które wspierają struktury państwa w przypadku konfliktu w cyberprzestrzeni. Do kluczowych pól działań cywilnych obrońców cyberprzestrzeni zaliczyć można:

a) obszary propagandowe;
b) ataki na infrastrukturę krytyczną;
c) ataki skierowane na istotne serwisy masowe (w tym bankowość elektroniczną).

Należy pamiętać, że współpraca osób cywilnych, zaangażowanych w ochronę państwa z pobudek głównie patriotycznych nie będzie możliwa bez kompatybilnej współpracy w strukturze cyberbezpieczeństwa (*Polska Obywatelska*...).

Zdolność do działania w cyberprzestrzeni jest możliwa przy relatywnie niskich kosztach. Budowanie zaawansowanych oddziałów ochrony w sieci, w porównaniu na przykład do ponoszonych kosztów związanych z budowaniem arsenału pancernego bądź floty powietrznej, jest tanie. Relacja między wydatkami na narzędzia informatyczne a specjalistami od bezpieczeństwa informatycznego jest niewielka, przyjmując, że są oni zatrudnieni jako pracownicy etatowi. Inwestycja w bezpie-

czeństwo cyberprzestrzeni to w dużej mierze inwestycja w kompetencje odpowiednich osób i dawanie im pola do działania, częściowo także wzajemnego zaufania państwa i obywateli, budowanie pozytywnych relacji.

W niektórych warunkach społeczno-ekonomicznych atrakcyjna staje się współpraca polegająca na wsparciu regularnych sił państwowych ochotniczymi oddziałami specjalistów, którzy zdolni są do prowadzenia działań związanych z bezpieczeństwem w cyberprzestrzeni.

Podobne rozwiązania stosuje się na całym świecie. Działanie specjalistów cyberbezpieczeństwa można ująć w trzech modelach:

a) *state-sponsored* – tak zwany model sponsorowany przez państwo. Oddziały, które działają w jego ramach mają bardzo nieregularną strukturę, o ile w ogóle ją posiadają. Specjaliści są angażowani przez państwo na zasadzie zlecenia pojedynczych zadań;
b) formalnego wsparcia sił zbrojnych – niektóre z państw w ramach sił zbrojnych wykorzystują wiedzę i zdolności cywili, na co dzień cenionych pracowników prywatnych firm lub instytucji, urzędników, prawników i tak dalej. Takie osoby częściowo działają jako ochotnicy, częściowo natomiast są powoływani w szeregi armii i odpowiednio przez nią opłacani;
c) ligi obrony cyberprzestrzeni – to model, który jest najbardziej obywatelskim i ochotniczym przedsięwzięciem związanym z cyberbezpieczeństwem danego kraju.

W 2016 roku działalność rozpoczęła ochotnicza grupa hakerów, której celem jest dbanie o bezpieczeństwo Polski w cyberprzestrzeni. Eksperci Polskiej Obywatelskiej Cyberobrony przeprowadzili szereg szkoleń (pierwszy raz w historii kraju) w zakresie cyberobrony terytorialnej. Poza tym o samej organizacji niewiele wiadomo, głównie ze względu na profil jej działania – anonimowość hakerów. W Polsce istnieje coraz więcej nastawionych patriotycznie grup, które specjalizują się w dbaniu o bezpieczeństwo teleinformatyczne. Polska Obywatelska Cyberobrona jest stowarzyszeniem oficjalnie zatwierdzonym przez Ministerstwo Obrony Narodowej. Ta niewielka grupa łączy w sobie nie tylko programistów, ale i dziennikarzy, i prawników, i tak dalej. Kontaktują się oni ze sobą za pomocą łączy internetowych, ponieważ nie wszyscy mieszkają w Polsce.

Bezpieczeństwo cyberprzestrzeni staje się priorytetem nie tylko dla władz państw, ale również dla obywateli, w tym przypadku wyszkolonych pod kątem ochrony przestrzeni wirtualnej. Wciąż zachodzi zmiana

w postrzeganiu cyberprzestrzeni, coraz częściej można w niej znaleźć odwołania do świata materialnego i powiązań pomiędzy tymi światami. Z jednej strony więcej osób może jej zagrozić, z drugiej natomiast cyberprzestrzeń zyskuje coraz więcej obrońców – patriotów, którzy czują się zobowiązani być częścią obrony terytorialnej w granicach Internetu. Osoby te motywowane są najczęściej oddaniem własnej ojczyźnie i szacunkiem do środowiska hakerskiego, ponieważ posiadając niezwykłe umiejętności informatyczne pozostają anonimowi, przedkładając ambicje i umiejętności nad służbę krajowi.

Bibliografia

Castells M. (2003), *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*, Dom Wydawniczy Rebis, Poznań.

Castells M. (2010), *Społeczeństwo sieci*, Wydawnictwo Naukowe PWN, Warszawa.

Cywilni eksperci powołają Polską Obywatelską Cyberobronę (2015), http://www.pap.pl/z-zycia-pap/news,402223,cywilni-eksperci-powolaja-polska-obywatelska-cyberobrone.html, 14.12.2017.

Maj M. (2014), *Cyberarmia ochotników*, https://www.cybsecurity.org/wp-content/uploads/2013/04/ciip-focus-8.pdf, 14.12.2017.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej (2015), Biuro Bezpieczeństwa Narodowego, Warszawa.

Du Vall M. (2014), *Infoaktywizm. Strategie komunikacyjne społeczników ery cyfrowej*, w: *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja)*, red. Maria Marczewska-Rytko, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin.

Gorzelak K., Jacewicz P. (2012), *Bezpieczeństwo w cyberprzestrzeni*, Infos, Biuro Analiz Sejmowych, nr 10 (124).

Góra J. (2015), *Cyberprzestępczość – hacting/cracking*, https://magazyn.mediarecovery.pl/cyberprzestepczosc-hacking-cracking/, 10.12.2017.

Hackerzy, Crackerzy i inni nie zawsze negatywni bohaterowie Internetu, http://www.heuristic.pl/blog/internet/Hackerzy-Crackerzy-i-inni-nie-zawsze-negatywni-bohaterowie-Internetu;144.html, 11.12.2017.

Hofmokl J. (2009), *Internet jako nowe dobro wspólne*, Wydawnictwo Akademickie i Profesjonalne, Warszawa.

Kaczmarek S. (2014), *Wpływ cyberprzestępczości na światową gospodarkę*, www.it-polska-news.pl/raport-bezpieczenstwo/wplyw-cyberprzestepczosci-na-swiatowagospodarke, 12.12.2017.

Katalog zagrożeń, cert.gov.pl.

Krasnodębski G. (2008), *Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego*, http://www.uwm.edu.pl/.../42_, 28.11.2017.

Madej M. (2009), *Rewolucja informatyczna- istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Polski Instytut Spraw Międzynarodowych, ss. 17–40.

Michalik Ł., *Haker, cracker, phreaker. Czym różnią się od siebie sieciowi przestępcy?*, https://gadzetomania.pl/11106,haker-cracker-phreaker-czym-roznia-sie-od-siebie-sieciowi-przestepcy, 11.12.2017.

Mikko Hypponen: Polska jest celem cyberprzestępców, to geopolityka, http://www.cyberdefence24.pl/703504,mikko-hypponen-polska-jest-celem-cyberprzestepcow-to-geopolityka, 13.12.2017.

Polska Obywatelska Cyberobrona. Cyberarmia Ochotników, https://www.cybsecurity.org/pl/cyberarmia-ochotnikow/#more-5499, 14.12.2017.

Reguła G. (director) (2014), *Tajemniczy świat informacji w pigułce*, cz. I, https://www.youtube.com/watch?v=oi4b8MUGzbU, 28.11.2017.

Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, Warszawa 2010.

Surgut K. (2017), *Haker… ma wiele odmian*, http://krzysztofsurgut.innpoland.pl/133721,haker-ma-wiele-odmian, 11.12.2017.

Szulc-Wałecka E. (2014), *Znaczenie cyberterroryzm we współczesnym świecie*, w: *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja)*, red. M. Marczewska-Rytko, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin.

Ustawa z 27 lipca 2001 roku *o ochronie baz danych*, Dz. U. 2001, Nr 128, poz. 1402.

Ustawa z 18 lipca 2002 roku *o świadczeniu usług drogą elektroniczną*, Dz. U. 2002, Nr 144, poz. 1204.

Ustawa z 16 lipca 2004 roku *Prawo telekomunikacyjne*, Dz. U. 2004, Nr 171, poz. 1800.

Ustawa z 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*, Dz. U. 2007, Nr 89, poz. 590.

Hackers in the service of the state – virtual side of patriotism

Summary

In recent times, the cyberspace fonctions as the alternative to the physical world. Each of our actions can be reflected in the virtual world, like it's been happening for several decades already when it comes to negative phenomena like crime or fights in a broad context. The network society pays special attention to the flow of information, which is a valuable good in the face of an overload of useless knowledge. Those who have

information and know how to use it properly are the ones in chargé. The article deals with the influence of work and hacker's involvement on the state safety and motivation of their behavior.

Key words: hacker, cybersecurity, patriotism

Informacja o autorze

Faustyna Kowalska – doktorantka w Zakładzie Badań Władzy Lokalnej i Samorządu na Wydziale Nauk Politycznych i Dziennikarstwa. Sekretarz Koła Naukowego Nauki o Bezpieczeństwie. Obszar zainteresowań to głównie rozwój inteligentnych miast, wpływ nowoczesnych technologii na rozwój państw, cyberbezpieczeństwo.