Andrzej Kozłowski

Uniwersytet Łódzki
andrzejk1234@gmail.com

Bezpieczeństwo cybernetyczne w strategicznych dokumentach Wielkiej Brytanii 2009–2011

Streszczenie: Niniejszy artykuł stara się odpowiedzieć na pytanie o rolę i miejsce cyberbezpieczeństwa w najważniejszych dokumentach strategicznych Wielkiej Brytanii w latach 2009–2011. Cyberprzestrzeń odgrywa coraz istotniejszą rolę dla sprawnego funkcjonowania państwa i jego społeczeństwa i dlatego zapewnienie bezpieczeństwa w sferze wirtualnej jest tak istotne. W artykule przeanalizowano zapisy strategii bezpieczeństwa narodowego z tamtego okresu jak również strategii cyberbezpieczeństwa. Opisano najważniejsze priorytety, sposoby ich osiągnięcia oraz rolę instytucji, które są odpowiedzialne za zabezpieczenie sieci teleinformatycznych Wielkiej Brytanii. Przy analizie strategii bezpieczeństwa narodowego wskazano rolę, jaką odgrywa w nich cyberbezpieczeństwo. Dokonano szczegółowej oceny oraz przeprowadzono analizę porównawczą wyżej wymienionych dokumentów.

Wzrost roli bezpieczeństwa teleinformatycznego

Gwałtowna informatyzacja świata, która rozpoczęła się na początku lat dziewięćdziesiątych spowodowała wzrost znaczenia cyberprzestrzeni¹ dla bezpieczeństwa państwa. Obecnie pełni ona rolę kręgosłupa współczesnego społeczeństwa, stanowiąc integralną część gospodarki oraz mając kluczowe znaczenie dla funkcjonowania współczesnego państwa. Wśród wielu zalet takiej sytuacji można wymienić uproszczenie i wynikające z tego przyspieszenie działania instytucji państwowych. Z drugiej strony nowa technologia

¹ „Cyberprzestrzeń jest domeną fizyczną będącą wynikiem utworzenia systemów informacyjnych i sieci, które umożliwiają wzajemne oddziaływanie drogą elektroniczną” (Rattray J. Gregory, 2004: 30).

to nie tylko nowe szanse, ale również niespotykane wcześniej zagrożenia, takie jak złośliwe oprogramowanie, czy ataki hakerskie, w wyniku których można utracić cenne dane. Rosnąca rola cyberprzestrzeni, jako fundamentu współczesnego świata wynika z upowszechnienia Internetu, który z niewielkiej sieci łączącej ośrodki uniwersyteckie w Stanach Zjednoczonych stał się globalną siecią komputerową. Tę zmianę najlepiej oddają statystyki, wskazując, że na początku lat dziewięćdziesiątych na świecie było 16 milionów internautów, a obecnie ich liczba przekroczyła 2 miliardy. „Usieciowienie” świata stale wzrasta, a według prognoz w 2015 roku liczba połączonych ze sobą urządzeń elektronicznych ma przekroczyć liczbę ludzi na kuli ziemskiej (*World Internet Users and Population Stats*). Prowadzi to do jednoczesnego wzrostu liczby cyberszpiegów i cyberprzestępców, jak również zwiększenia liczby państw prowadzących coraz bardziej agresywną działalność w cyberprzestrzeni. Niski koszt dokonywania ataków oraz względna anonimowość zachęcają potencjalnych przestępców do działania.

Corocznie, działalność cyberprzestępców powoduje straty finansowe rzędu biliona dolarów na całym świecie (Florêncio Dinei, Herley Cormac). Kradną oni własność intelektualną, wrażliwe informacje komercyjne i państwowe. Co więcej, niektóre państwa uzyskały zdolność do prowadzenia cyberwojny, czego przykładem mogą być ataki: na Estonię w 2007 roku (Traynor Ian) i na Gruzję w 2008 (Korns W. Stephen, Kastenber E. Joshua. 2008–2009: 61–76). Ostatnio wirus Stuxnet pokazał, że możliwe jest uszkodzenie fizycznej infrastruktury – irańskich wirówek do wzbogacania uranu – poprzez zastosowanie szkodliwego programu komputerowego (Sanger, 2012: 188–226).

Znaczenie cyberprzestrzeni dla Wielkiej Brytanii

Wielka Brytania mimo swojego dogodnego, wyspiarskiego położenia narażona jest na ataki cybernetyczne, jak każde inne państwo na świecie. Charakter cyberprzestrzeni powoduje, że naturalne bariery takie jak morza i oceany ułatwiające obronę na tradycyjnym polu walki nie mają wpływu na rzeczywistość wirtualną. Naturalne bariery wodne, które skutecznie chroniły Wielką Brytanię przed najeźdźcami, w cyberprzestrzeni nie mogą skutecznie spełniać swojej roli.

Brytyjczycy zaliczają się do istotnych graczy na arenie międzynarodowej, są członkiem m.in. NATO i Unii Europejskiej. Jedno z głównych centrum światowych finansów – angielskie *City* ulokowane jest w tym kraju. Co więcej, Wielka Brytania jest jednym z najbardziej zelektronizowanych krajów na kuli ziemskiej – ponad 30 milionów Brytyjczyków codziennie korzysta z Internetu. Są oni narażeni na ataki cybernetyczne, nie będąc nawet świadomym zagrożenia (*Office for National Statistics*).

Dla brytyjskiej gospodarki zapewnienie cyberbezpieczeństwa jest nie do przecenienia. Wyliczono, że rynek internetowy wart jest ponad 80 miliardów funtów, co stanowi około 5,6% brytyjskiego Produktu Krajowego Brutto. Wielka Brytania jest też krajem w Europie z największą liczbą osób dokonujących zakupów przez Internet, czyni to ponad 70% obywateli (Guy Laurence). Statystyki te jasno pokazują wartość sektora informatycznego dla Brytyjczyków i jednoznacznie wskazują, że zapewnienie mu bezpieczeństwa leży w żywotnym interesie Brytyjczyków. Niestety wraz ze wzrostem ilości użytkowników Internetu w Wielkiej Brytanii, rośnie aktywność cyberprzestępców. Z powodu ich działalności notowane są straty rzędu 27 miliardów funtów (*The Cost of Cybercrime*), a coraz częściej atakowane są systemy komputerowe i sieci elementów infrastruktury krytycznej, takie jak elektrownie, lotniska. Szacuje się, że ponad 2/3 usługodawców odpowiedzialnych za jej działalność była celem ataków z wykorzystaniem szkodliwego oprogramowania. Udany atak hakerski na infrastrukturę krytyczną grozi paraliżem funkcjonowania obecnego społeczeństwa. Operacja taka może zostać przeprowadzona np. z wykorzystaniem poczty elektronicznej. W ciągu miesiąca migruje ponad 20 tys. wiadomości zawierających szkodliwe oprogramowanie, z czego ponad 1 tys. z nich wysyłanych jest celowo. Liczba ta zwiększyła się z porównaniu z rokiem ubiegłym (*In the Dark*).

Strategia cyberbezpieczeństwa 2009

Rosnące zagrożenie w cyberprzestrzeni zmusiło brytyjski rząd do strategicznego podejścia do tej problematyki. Kwestie te zostały wspomniane w strategii bezpieczeństwa Wielkiej Brytanii z 2009 roku. W dokumencie tym poświęcono im tylko dwie strony. Jednym z najważniejszych punktów była zapowiedź opublikowania w tym samym roku pierwszej kompleksowej strategii poświęconej temu zagrożeniu. Ponadto zdecydowano o powołaniu Biura Cyberbezpieczeństwa, którego głównym zadaniem miało być koordynowanie działań w cyberprzestrzeni oraz opracowywanie nowych strategii. Stworzono też Centrum Operacji Cybernetycznych do monitorowania sytuacji w cyberprzestrzeni, lepszego zrozumienia natury ataków, które są wymierzone w Wielką Brytanię oraz zapewnienia łatwego dostępu do szeroko dostępnej informacji dla sektora prywatnego i publicznego (*The National Security strategy of the United Kingdom*, 2009: 102–104). Centrum to mieści się w Cheltenham i jest jednym z elementów Centrali Łączności Rządowej (GCHQ), która jest brytyjską służbą specjalną zajmującą się wywiadem elektronicznym i odpowiedzialna jest za zbieranie i analizę informacji pochodzących m.in. z cyberprzestrzeni (*Keeping our Society Safe and Successful in the Internet Age*). Zarysowano też strategię, której trzy

główne cele miały polegać na zmniejszeniu ryzyka w cyberprzestrzeni, efektywniejszym jej wykorzystaniu do własnych celów oraz edukowaniu ludzi w kwestii bezpiecznego jej użytkowania (*The National Security Strategy of the United Kingdom*, 2009: 102–104).

Temat bezpieczeństwa w cyberprzestrzeni został rozwinięty w pierwszej kompleksowej strategii cyberbezpieczeństwa zatytułowanej „Strategia cyberbezpieczeństwa. Bezpieczeństwo, ochrona i odporność w cyberprzestrzeni” opublikowanej w 2009 roku. Zostały w nim zdefiniowane trzy grupy, które stanowią największe zagrożenie dla Wielkiej Brytanii. Pierwszą z nich są cyberkryminaliści i zorganizowane cybergangi, które nie tylko mogą zarażać komputery szkodliwym oprogramowaniem, ale również manipulować użytkownikami sieci. Jako poważne zagrożenie płynące ze strony tych grup wymieniono zjawisko phishingu², kradzieży kart kredytowych, oszustw na aukcjach internetowych czy w grach online. Problem ten, w takim samym stopniu dotyczy dużych przedsiębiorstw, jak indywidualnych użytkowników Internetu (*Cyber Security Strategy of the United Kingdom*, 2009: 13).

Drugą grupą, uważaną za zdecydowanie groźniejszą są państwa, zdolne do przeprowadzenia skoordynowanych ataków w cyberprzestrzeni. Według autorów strategii mogą one przeprowadzać operację dezinformujące oraz zakłócać działania infrastruktury krytycznej. Dokument definiuje też narzędzia, którymi mogą posługiwać się hakerzy na usługach innych krajów, wskazując na programy, które niepostrzeżenie instalują się na komputerach i czekają na sygnał do uruchomienia (*Cyber Security Strategy of the United Kingdom*, 2009: 13).

Trzecią grupą, która stanowi dla Wielkiej Brytanii zagrożenie są terroryści. Sposób wykorzystania przez nich cyberprzestrzeni różni się od wcześniejszych dwóch przypadków. Według tego strategicznego dokumentu, używają oni Internetu głównie do koordynowania działań, szerzenia radykalnej ideologii, zbierania funduszy, a nie do przeprowadzania ataków. Autorzy wskazują, że może to w niedalekiej przyszłości ulec zmianie, ale obecnie terroryści preferują uderzenia klasyczne, ponieważ są zdecydowanie bardziej spektakularne (*Cyber Security Strategy of the United Kingdom*, 2009: 13).

Najważniejszym elementem strategii z roku 2009 były sugerowane kroki, które brytyjski rząd powinien podjąć w celu przeciwdziałaniu zagrożeniom. Wskazywano tutaj na konieczność wielopłaszczyznowego podejścia obejmującego ścisłą współpracę rządu, sektora prywatnego oraz środowisk

² *Phishing* to zjawisko polegające na wyłudzeniu poufnych informacji, haseł lub szczegółów karty kredytowej, poprzez podszywanie się po godną zaufania osobę lub instytucję publiczną (*Phishing* – łowienie naiwnych).

naukowych. Podkreślono również konieczność kooperacji z międzynarodowymi partnerami. Tylko w ten sposób, według autorów strategii, można zminimalizować zagrożenia płynące z cyberprzestrzeni, która nie posiada żadnych, ani państwowych ani naturalnych barier, a atak wymierzony w Wielką Brytanię może zostać przeprowadzony z komputerów znajdujących się na całym świecie (*Cyber Security Strategy of the United Kingdom*, 2009: 15–16).

W strategii poświęcono też nieco miejsca na działania ofensywne. Autorzy dokumentu zauważyli, że cyberprzestrzeń może być wykorzystywana do walki z przestępcami i terroryzmem, a nawet przez wojsko, ale aspekt ten w dokumencie nie został rozwinięty (*Cyber Security Strategy of the United Kingdom*, 2009: 14).

Podsumowując, strategia bezpieczeństwa narodowego z 2009 roku razem z pierwszą strategią cyberbezpieczeństwa zawierały głównie ogólne stwierdzenia wskazujące na rosnące zagrożenia związane z działalnością hakerów, akcentowały konieczność współpracy sektora publicznego i prywatnego, oraz międzynarodowej kooperacji. Dużo miejsca poświęcono na opisy zagrożeń i sposobu działań hakerów, ale zabrakło podania konkretnych rozwiązań danych problemów, jak również wyznaczenia długoterminowych celów. Jedynym rzeczywistym osiągnięciem obu strategii było powołanie do życia Biura Cyberbezpieczeństwa i Centrum Operacji Cybernetycznych. Nawet, jednak w przypadku tych dwóch instytucji, eksperci zgłosili wiele zastrzeżeń. Według nich nie określono ich budżetu, miejsca w brytyjskim systemie legislacyjnym, nie odpowiadano na pytanie czy mogą one wpływać na uchYLENIE umów zawartych przez rząd, które narażają na szwank cyberbezpieczeństwo kraju. Większość ze specjalistów negatywnie oceniało strategię, wskazując, że stworzyły one kolejne dwa ciała odpowiedzialne za cyberprzestrzeń, które zamiast wzmocnić efektywność działań tylko i wyłącznie przyczynią się do zwiększenia biurokracji (*UK Cyber Security Strategy – Even More Bureaucracy, but No Financial Budget, Legislative Power or Democratic*). Z drugiej jednak strony należy pamiętać, że opracowana strategia w cyberprzestrzeni była pierwszą w dziejach Wielkiej Brytanii i jedną z pierwszych na świecie. Wyznaczać miała główne trendy w dziedzinie bezpieczeństwa cybernetycznego, a nie proponować konkretne rozwiązania.

Nowy rząd – nowe pomysły

Dojście do władzy nowego rządu Davida Camerona wpłynęło na zmianę podejścia do problemu cyberbezpieczeństwa w Wielkiej Brytanii. Było to już widoczne w publikowanych w 2010 roku strategii bezpieczeństwa narodowego oraz strategicznym przeglądzie bezpieczeństwa. Już sama jej

nazwa „Silna Wielka Brytania w świecie zaskakujących zmian” wskazuje na zwrócenie uwagi na dynamikę zmian zachodzących w obecnym świecie stosunków międzynarodowych i związanego z tym paradygmatu bezpieczeństwa. We wstępie napisano, że obecny stan bezpieczeństwa państwa jest najwyższy w historii, ale zarazem podkreślono wrażliwość na nowe zagrożenia asymetryczne. Oznacza to, że obecnie nie występuje groźba ataku przez obce siły na terytorium Wielkiej Brytanii, z drugiej jednak strony niesamowita otwartość i usieciowienie współczesnego brytyjskiego społeczeństwa czyni je podatniejszym na nowe zagrożenia (*A Strong Britain in an Age of Uncertainty: The National Security Strategy*).

W nowej strategii bezpieczeństwa znalazła się krytyka poprzedniego rządu, zarzucająca mu anachroniczne podejście do problematyki bezpieczeństwa państwa. Głównym zarzutem sformułowanym pod adresem poprzedniej ekipy rządzącej było korzystanie z nieprzystającego do współczesnych warunków, przeglądu bezpieczeństwa z roku 1998 roku (Stachowski, 2010: 505).

Z perspektywy cyberbezpieczeństwa, nowa strategia narodowa była innowacyjna, ponieważ na pierwszym miejscu zagrożeń umieszczono ataki cybernetyczne ze strony państw lub zorganizowanych grup przestępczych. Tym samym rząd brytyjski uznał niebezpieczeństwo płynące z ich strony za równie ważne co terroryzm międzynarodowy, poważne katastrofy nuklearne i międzynarodowy kryzys militarny (*A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2010: 27).

Z punktu widzenia cyberbezpieczeństwa, godnym odnotowania zapisem jest ten mówiący o położeniu szczególnego nacisku na przygotowanie się do odparcia potencjalnych ataków aktorów niepaństwowych, i to nie w klasycznym środowisku, ale w tzw. czwartym wymiarze czyli cyberprzestrzeni. W celu odpowiedniego przygotowania na to wyzwania sugeruje się konieczność prowadzenia symulacji oraz tworzenia scenariuszy reagowania na pojawiające się zagrożenia (Stachowski, 2010: 506).

Przyjmując założenie, że strategia jest mało wartościowa bez narzędzi wprowadzających, rząd podjął decyzję o opublikowaniu strategicznego przeglądu bezpieczeństwa (Stachowski, 2010: 502). Zagrożenia w cyberprzestrzeni zostały w nim zidentyfikowane jako zagrożenia pierwszoplanowe, które mogą mieć wpływ na Internet, sieci teleinformatyczne i systemy komputerowe Wielkiej Brytanii. Na poprawienie sytuacji, rząd przeznaczył 650 milionów funtów, mimo kryzysu gospodarczego i związanych z tym cięć w finansach publicznych, w tym brytyjskim Ministerstwie Obrony. W przeciągu czterech lat zaplanowano stworzenie jednego punktu kontaktowego, gdzie obywatele i przedsiębiorcy będą mogli zgłaszać cyberprzestępstwa; wprowadzenie nowego programu szkoleniowego, którego charakter ukierunkowany jest na poprawienie kompetencji specjalistów w dziedzinie walki w cyberprzestrzeni; utworzenie szerokiego monitoringu

dostarczanych produktów i usług informatycznych, w szczególności systemów adresowanych do wojska; zwiększenie inwestycji w narodowy potencjał wywiadowczy, a zwłaszcza w Centrum Operacji Bezpieczeństwa Cybernetycznego w GCHQ (połowa z 650 milionów ma zostać przeznaczona właśnie na tę instytucję, która ma odgrywać główną rolę w cyberobronie Wielkiej Brytanii); udoskonalenie systemu identyfikacji luk w cybernetycznej infrastrukturze krytycznej państwa, mającego umożliwić ich szybkie wykrycie i usunięcie; stworzenie Grupy Działań Obrony Cybernetycznej Państwa, która będzie głównym narzędziem Ministerstwa Obrony w cyberprzestrzeni, odpowiedzialnym za ochronę systemów jak również opracowanie możliwości przeprowadzenia ataków; zacieśnienie współpracy z partnerami zagranicznymi co do wymiany danych i planów oraz podejmowanie wspólnego działania w celu wypracowania wspólnych standardów oraz podstawowych norm w zakresie cyberbezpieczeństwa; edukowanie i uświadamianie społeczeństwa w zakresie bezpiecznego użytkowania Internetu (m.in. poprzez rozwój portali *Get Safe Online*³ i *Get Security Challenge*⁴); współpracę z sektorem prywatnym i ośrodkami naukowymi, w celu udoskonalenia możliwości odpowiedzi na wyzwania w cyberprzestrzeni oraz opracowania dalekosiężnych planów i strategii (*Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 2010: 48–50).

Stratega bezpieczeństwa narodowego i strategiczny przegląd bezpieczeństwa z 2010 roku uczyniły z zagrożeń cybernetycznych jedno najpoważniejszych wyzwań dla obronności tego państwa. Zasugerowano konkretne rozwiązania, które zostały rozwinięte w strategii cyberbezpieczeństwa. Najważniejszym aspektem strategicznego przeglądu było określenie dokładnych ram finansowych, które przeznaczone są na reformę cyberobrony.

³ Omawiając bezpieczeństwo cybernetyczne Wielkiej Brytanii nie można zapominać o inicjatywie *Get Safe Online*, która powstała w 2005 roku. Jest to portal internetowy stworzony we współpracy sektora publicznego i prywatnego, którego głównym zadaniem jest podniesienie świadomości o bezpiecznym korzystaniu z Internetu. Inicjatywa adresowana jest głównie do indywidualnych użytkowników sieci, jak również małych przedsiębiorstw, które mogą nie posiadać odpowiednich funduszy, żeby zatrudnić specjalistów od bezpieczeństwa cybernetycznego. *Get Safe Online* współpracuje z rządem, jak również najważniejszymi firmami sektora prywatnego, odpowiedzialnymi za bezpieczeństwo cybernetyczne. Oferta portalu jest bardzo szeroka i obejmuje narzędzia do zwalczania złośliwego oprogramowania, najnowsze wersje programów zabezpieczających, jak również informacje odnośnie bezpiecznego poruszania się w sieci. (*The Rough Guide to Online Safety*, 2011).

⁴ *Get Security Challenge* są to zawody w cyberprzestrzeni organizowane przez brytyjski rząd, których głównym celem jest znalezienie wybitnych osób, zajmujących się bezpieczeństwem cybernetycznym. Hakerzy zgłaszają chęć udziału w zawodach, które polegają na łamaniu przykładowych zabezpieczeń. Najlepsi z uczestników mogą liczyć nawet na pracę w instytucjach państwowych. Szerzej na ten temat patrz: (*Cyber Security Challenge UK*).

„Strategia cyberbezpieczeństwa Wielkiej Brytanii. Ochrona i wsparcie dla Wielkiej Brytanii w cyfrowym świecie”

Jeden z zapisów strategii bezpieczeństwa narodowego z 2010 roku mówił o stworzeniu nowej osobnej strategii cyberbezpieczeństwa. Wynikało to z faktu, że poprzedni dokument był krytykowany i nie spełniał oczekiwań. Nowa strategia została opublikowana pod tytułem „Strategia Cyberbezpieczeństwa Wielkiej Brytanii. Ochrona i wsparcie dla Wielkiej Brytanii w cyfrowym świecie”.

Twórcy dokumentu zaznaczyli, że w zglobalizowanym świecie nie można mówić o czymś takim jak absolutne bezpieczeństwo w cyberprzestrzeni. Zaproponowano podejście polegające na minimalizacji ryzyka. Słusznie dostrzeżono, że rząd Wielkiej Brytanii ma ograniczone pole manewru w cyberprzestrzeni z dwóch powodów: jest ona w dużej części używana przez sektor prywatny oraz ma charakter transnarodowy. Stąd też wynika potrzeba pracy z przedsiębiorstwami oraz partnerami międzynarodowymi. (*Securing Britain in an Age of Uncertainty: The Strategic Defense and Security Review*, 2010: 48–50).

Kluczowym aspektem nowego dokumentu była wizja Wielkiej Brytanii w 2015 roku jako państwa, które czerpie zyski, zarówno ekonomiczne jak i społeczne z bezpiecznego użytkowania cyberprzestrzeni. Jednocześnie zapisy legislacyjne, regulujące zachowanie użytkowników Internetu mają być przejrzyste i klarowne i nader wszystko szanować brytyjskie przywiązanie do wolności (*The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital Word*, 2011: 8). W 2015 roku Wielka Brytania ma być w stanie przeprowadzić działania ofensywne w odpowiedzi na zagrożenia w cyberprzestrzeni. Według autorów dokumentu, każdy Brytyjczyk ma mieć możliwość dostępu do cyberprzestrzeni, która jest wykorzystywana do szerzenia tolerancji i szacunku dla odmienności kulturowych. W 2015 roku ma być to miejsce otwarte, ze swobodą przepływu informacji i poszanowaniem własności prywatnej (*The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital Word*, 2011: 8).

Autorzy dokumenty przewidują, że w 2015 roku brytyjscy użytkownicy Internetu będą posiadać podstawową wiedzę na temat zagrożeń w cyberprzestrzeni oraz mieć możliwość swobodnego dostępu do informacji na temat najnowszych szkodliwych programów. Nacisk położono również na bezpieczne przesyłanie informacji i wrażliwych danych. Co więcej, brytyjski użytkownik Internetu ma posiadać zdolność identyfikacji zagrożeń, które będzie zgłaszał w odpowiednim miejscu (*The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital Word*, 2011: 31).

Dokument wyznacza również rolę dla przedsiębiorców, którzy w 2015 mają być świadomi zagrożeń w cyberprzestrzeni. Ma to doprowadzić do

sytuacji, w której wrażliwe informacje są przekazywane z zachowaniem należytych środków bezpieczeństwa. Bliska współpraca sektora prywatnego z publicznym, poprzez wymianę wartościowych danych, ma przyczynić się do skutecznego zwalczania zagrożeń cybernetycznych. Autorzy dokumentu liczą, że prywatny kapitał zainwestuje w stworzenie wielu ośrodków doskonalenia umiejętności bezpiecznego użytkowania w cyberprzestrzeni.

W 2015 roku rząd ma posiadać zdolności pozwalające na wykrywanie i zwalczanie najgroźniejszych ataków cybernetycznych, a jego infrastruktura ma się cechować zmniejszoną podatnością na ataki. Ma to być możliwe dzięki wykształceniu odpowiedniej kadry specjalistów oraz dzięki skutecznej wymianie informacji z ośrodkami naukowymi i przemysłowymi. Autorzy dokumentu liczą również na owocną współpracę z partnerami międzynarodowymi co pozwoli ukształtować pewne normy zachowań w cyberprzestrzeni oraz wzmocnić reguły prawne (*The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital Word*, 2011: 23).

Zagrożenia według strategii bezpieczeństwa cybernetycznego z 2011 roku

Większość zagrożeń wymienionych w nowym dokumencie powtarza zapisy strategii z 2009 roku. Nowym elementem jest tutaj „haktywizm”, czyli forma internetowego protestu społecznego. Według autorów dokumentu, osoby uprawiające tego typu działalność w sieci, swoimi akcjami często powodują finansowe straty lub sieją zamęt. Innym trendem poruszoną w dokumencie jest wzrost liczby szkodliwego oprogramowania do smartfonów z 600 programów w 2009 roku do ponad 1200 w 2011. Wzrastająca liczba użytkowników tych urządzeń mobilnych, szczególnie wśród przedsiębiorców, nakazuje wprowadzenie odpowiednich środków zapobiegawczych, jednak te nie zostały w strategii sprecyzowane. Wśród zagrożeń wymienia się też sytuację, w której społeczeństwo straci zaufanie do możliwości bezpiecznego używania Internetu.

Główną przeszkodą w zagwarantowaniu bezpieczeństwa w cyberprzestrzeni jest kwestia ograniczenia wolności w Internecie. Z jednej strony istnieje duża szansa, że przyczyni się to do faktycznego poprawienia bezpieczeństwa, z drugiej jednak może doprowadzić do protestów społecznych i uczynić rząd przeciwnikiem społeczeństwa, a nie gwarantem jego bezpieczeństwa. Władze Wielkiej Brytanii starają się doprowadzić do poprawienia zabezpieczenia cyberprzestrzeni, ale bez ingerencji w życie prywatne obywateli (*The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital Word*, 2011: 16).

Wśród problemów z zagwarantowaniem cyberbezpieczeństwa, jako jeden z najpoważniejszych, wymieniono fakt, że większość cyberprzestrzeni jest głównie użytkowana przez prywatnych użytkowników. Składa się ona z wielu fizycznych elementów sprowadzanych z całego świata, od różnych dostawców, którzy często nie są w żaden sposób sprawdzani. Może to prowadzić do sytuacji, w której niektóre przedsiębiorstwa celowo dostarczają wadliwe elementy infrastruktury, która jest bardziej podatna na atak (*The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World*, 2011: 18).

Drugim najpoważniejszym problemem w zagwarantowaniu cyberbezpieczeństwa jest niemożność określenia roli jaką cyberprzestrzeń ma odgrywać w przyszłości oraz zagrożenia, które mogą się pojawić. Tempo zmian zachodzących w tym środowisku powoduje, że obecnie istniejąca obrona może okazać się w niedalekiej przyszłości niewystarczająca i przestarzała.

Sposób realizacji wizji zagwarantowania bezpieczeństwa cybernetycznego Wielkiej Brytanii w 2015 roku

W drodze do zrealizowania wizji bezpieczeństwa cybernetycznego Wielkiej Brytanii w 2015 roku wyodrębniono 4 główne cele:

1. Skuteczne zwalczanie cyberprzestępczości i uczynienie z Wielkiej Brytanii najbezpieczniejszego miejsca na świecie do prowadzenia działalności gospodarczej w cyberprzestrzeni.

Cel ten ma zostać osiągnięty poprzez zmniejszenie podatności brytyjskich sieci na ataki, ograniczenie działalności cyberprzestępców oraz promocję skutecznego partnerstwa pomiędzy sektorami prywatnym i publicznym. Sugeruje się również konieczność zwiększenia świadomości społecznej na temat ataków, ulepszenie mechanizmu reagowania na zaistniałe incydenty, lepszą ochronę kluczowych informacji oraz usług, promowanie zaufania w cyberprzestrzeni. Strategia z 2011, w przeciwieństwie do poprzedniego dokumentu zawiera również dokładne działania, które powinny zostać podjęte. Autorzy sugerują następujące czynności:

- przejrzenie istniejących aktów legislacyjnych pod kątem ich przydatności do zwalczania cyberprzestępców,
- zachęcenie sądów do wymierzania odpowiednich kar cyberprzestępcom oraz usprawnienie działalności agencji ochrony porządku publicznego,
- stworzenie narodowej jednostki policji odpowiedzialnej za cyberprzestępstwa, jak również zachęcenie ekspertów do współpracy z nią,

- stworzenie jednego punktu informacyjnego w ramach polityki informacyjnej, gdzie przedsiębiorstwa i klienci indywidualni mogą zgłaszać cyberataki,
- podjęcie szeroko zakrojonych działań w celu zwalczania zbrodni niewiasty w Internecie. Proponuje się nałożenie sankcji na osoby ją propagujące,
- zacieśnianie współpracy z przedsiębiorstwami przy wdrażaniu nowego prawa, które ma nie przeszkadzać w swobodnej wymianie informacji, a zarazem przewidywać poważne kary dla cyberprzestępców,
- współpracę z międzynarodowymi organizacjami oraz innymi państwami w celu opracowywania i wdrażania trans-granicznych rozwiązań prawnych, które zapobiegą sytuacji tworzenia się bezpiecznych przystani dla cyberkryminalistów,
- praca z krajowymi, europejskimi i światowymi organizacjami w celu wypracowania jednolitych standardów bezpieczeństwa dla elementów fizycznych cyberprzestrzeni,
- budowa zaufanego partnerstwa pomiędzy sektorem prywatnym i publicznym w celu wzajemnego dzielenia się informacjami na temat zagrożeń, zwalczania incydentów, które zaistniały w cyberprzestrzeni, rozwijanie wzajemnych analiz trendów nowych zagrożeń oraz budowy potencjału i zdolności,
- zapewnienie wysokiego poziomu bezpieczeństwa cybernetycznego przy korzystaniu z usług publicznych online. Konsumenci muszą być pewni, że ich transakcje z rządem są należycie zabezpieczone,
- wsparcie dla brytyjskiego przemysłu produkującego fizyczne elementy cyberprzestrzeni,
- zapowiedziano również przeprowadzenie szczegółowych analiz dotyczących roli i szans przemysłu w pracy nad cyberbezpieczeństwem,
- rozwinięcie strategii marketingowej, która ma na celu promowanie zdolności brytyjskiego przemysłu w zapewnieniu bezpieczeństwa cybernetycznego,
- praca nad zwiększeniem świadomości wśród przedsiębiorców na temat zagrożeń płynących z cyberprzestrzeni oraz tego, jak można je zwalczać. Zalecenie dla nich, żeby współpracowali z dostawcami usług i towarów (*The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World*, 2011: 36–38).

2. Uczynienie z Wielkiej Brytanii bardziej odpornej na ataki cybernetyczne oraz zagwarantowanie skuteczniejszej obrony brytyjskich interesów w cyberprzestrzeni.

Rząd w realizacji tego długoterminowego celu postawił sobie za najważniejsze wzmocnienie obrony w cyberprzestrzeni oraz odporności na

ataki, jak również zmniejszenie siły ich oddziaływania oraz przeciwdziałania w celu wykorzystywaniu sieci przez terrorystów. Co więcej, zapowiedziano działania mające na celu udoskonalenie wykrywania zagrożeń w cyberprzestrzeni oraz wzmocnienie zdolności do powstrzymywania i neutralizowania ataków hakerskich. Szczegółowy plan akcji przedstawiony przez rząd Jej Królewskiej Mości zakłada:

- zacieśnienie współpracy z przedsiębiorstwami odpowiedzialnymi za kierowanie systemami krytycznej infrastruktury w celu zapewnienia bezpiecznego przekazu informacji,
- rozszerzenie opieki rządowej nad przedsiębiorstwami, które mają priorytetowe znaczenie dla brytyjskiej gospodarki,
- rzetelne sprawdzenie czy procedury odpowiedzi na zagrożenia w cyberprzestrzeni spełniają wymogi Unii Europejskiej i nie rzutują negatywnie na współpracę z międzynarodowymi partnerami,
- współpraca z sojusznikami w celu implementacji polityki bezpieczeństwa w cyberprzestrzeni opracowanej przez NATO,
- pracę nad efektywną strategią, która pozwoli na zakłócanie działalności radykałów w Internecie,
- zwiększenie potencjału przewidywania i zapobiegania wrogim aktom w cyberprzestrzeni (poprzez wymianę informacji pomiędzy sektorem prywatnym i publicznym, wzmocnienie obrony przeciwko atakom oraz skuteczne wykonywanie prawa, które pozwoli na ujęcie cyberkryminalistów),
- stworzenie Grup Operacyjnych w ramach Ministerstwa Obrony, które będą odpowiedzialne za integrację potencjałów cywilnych i wojskowych w cyberprzestrzeni (*The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World*, 2011: 39).

3. Praca nad rzecz kształtowania otwartej i stabilnej cyberprzestrzeni, która może być używana w bezpieczny sposób przez społeczeństwo Wielkiej Brytanii.

Rząd realizując ten cel zamierza oprzeć się na promowaniu otwartej i Inter-operacyjnej cyberprzestrzeni, gdzie zapewnienie bezpieczeństwa nie ma negatywnego wpływu na prawo wolności internautów. W szczegółowym planie działań wymieniono:

- kontynuowanie organizowania międzynarodowych konferencji poświęconych ustanowieniu międzynarodowych norm co do zachowania się w cyberprzestrzeni,
- przegląd istniejących przepisów dotyczących sektora komunikacyjnego w Wielkiej Brytanii,
- wsparcie dla idei otwartego Internetu,
- implementację bilateralnych, międzynarodowych porozumień ze Stanami Zjednoczonymi, Francją i Australią,

- szukanie porozumienia z państwami rozwijającymi się, które aktywnie angażują się w działalność w cyberprzestrzeni,
- aktywne zaangażowanie się w pracę międzynarodowych, jak i regionalnych organizacji, takich jak *Commonwealth*, Organizacja Bezpieczeństwa i Współpracy w Europie, Rada Europy i Międzynarodowy Związek Telekomunikacyjnym w celu zbudowania jednego modelu legislacyjnego definiującego zachowanie w cyberprzestrzeni,
- aktywne poszukiwanie w ramach dialogu bilateralnego i multilateralnego sposobu implementacji międzynarodowego prawa człowieka w cyberprzestrzeni,
- wzmocnienie światowego systemu poprzez budowanie zaufania pomiędzy głównymi aktorami działającymi w cyberprzestrzeni,
- współpraca w ramach UE z Komisją Europejską oraz Służbą Działań Zewnętrznych w celu stworzenia większej spójności w działaniach w cyberprzestrzeni,
- próby szukania porozumienia z dostawcami Internetu w celu współpracy w identyfikacji złośliwego oprogramowania (*The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital Word*, 2011: 39).

4. Wykształcenie wybitnych ekspertów w dziedzinie cyberbezpieczeństwa Wielkiej Brytanii.

Cel ten ma zostać osiągnięty przez stworzenie wspólnego programu badawczego, w ramach którego będą pracowali specjaliści z wielu dziedzin. Obejmować ma on działania mające na celu lepsze zrozumienie zagrożeń i ryzyka operowania w cyberprzestrzeni, jak również umożliwić łatwiejsze znalezienie wrażliwych punktów. Bardzo ważnym aspektem, dla autorów dokumentu jest uświadomieniu społeczeństwu ryzyka, jakie wiąże się z użytkowaniem cyberprzestrzeni. Nie można również zapominać o rozwijaniu technologicznych zdolności, które są kluczowe w zwiększaniu możliwości zapobiegania incydentom w cyberprzestrzeni. Autorzy dokumentu przygotowali szczegółowy plan, który obejmuje następujące punkty:

- zwiększenie zdolności przewidywania rozwoju technologicznego, proceduralnego i zachowania społecznego w cyberprzestrzeni,
- przeprowadzenie specjalnych programów adresowanych do uczniów jak i studentów,
- ustanowienie specjalnego programu, który miałby służyć za pole ćwiczeń do zwalczania zagrożeń w cyberprzestrzeni z rocznym budżetem 2 miliony funtów,
- zwiększenie kompetencji zawodowych osób odpowiedzialnych za bezpieczeństwo informacji oraz bezpieczeństwo cybernetyczne poprzez wprowadzenie jednego certyfikatu, potwierdzającego poziom zawansowania osób,

- wsparcie dla naukowców proponujących innowacyjne rozwiązania w cyberprzestrzeni,
- pomoc w rozwijaniu społeczności „etycznych hakerów”, którzy działali by w celu poprawy bezpieczeństwa cyberprzestrzeni,
- zachęcanie społeczeństwa do zgłaszania przypadków oszustw i kradzieży w Internecie z wykorzystaniem narzędzi „Action Fraud”,
- rozwijanie tzw. cyberhigieny, która miałaby polegać na edukacji społeczeństwa co do użytkowania Internetu w bezpieczny sposób i mogłaby przyczynić się do zredukowania liczby ataków o 80%,
- szerzenie wiedzy na temat bezpieczeństwa poprzez użycie mediów społecznościowych,
- stworzenie Centrum Doskonalenia Obrony Cybernetycznej podobnego do natowskiej instytucji znajdującej się w Estonii (*The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World*, 2011: 42).

Podsumowanie strategii

Nowa strategia bezpieczeństwa cybernetycznego została opracowana z uwzględnieniem głosów krytycznych w stosunku do poprzedniego dokumentu. Tym razem mamy do czynienia z przejrzystą wizją i długoterminowym celem, który brytyjski rząd zamierza osiągnąć. Stawiając sobie konkretne zadania do zrealizowania oraz podając konkretny termin, rząd będzie mógł łatwo ocenić sukcesy i porażki przy realizacji dokumentu. Sama strategia kładzie duży nacisk na czynnik ekonomiczny i społeczny, skupiając się na ochronie gospodarki i porządku społecznego. Czynnik militarny, wliczając w to zdolności ofensywne, po raz kolejny został zaniebdany. Niezwykle ciekawym, ale zarazem ryzykowanym pomysłem jest idea zaangażowania społeczności brytyjskiej w ochronę w cyberprzestrzeni. Według zapisów dokumentu, każdy obywatel, który korzysta z Internetu ma być elementem obrony cybernetycznej. Zaskoczeniem nie jest podkreślenie bliskiej współpracy między sektorem prywatnym a publicznym, ponieważ jest to cecha charakterystyczna dla wszystkich doktryn strategicznych mówiących o cyberbezpieczeństwie. Ważnym aspektem jest podkreślenie znaczenia jakości dostaw elementów fizycznych cyberprzestrzeni, ponieważ czynnik ten jest często niedoceniany, a może wiązać się z groźniejszymi konsekwencjami niż przy atakach z wykorzystaniem oprogramowania komputerowego. Wśród wad strategii trzeba zauważyć, zbyt dużą liczbę instytucji odpowiedzialnych za bezpieczeństwo cybernetyczne bez jednej koordynującej działalności pozostałych. Doprowadzi to do dublowania się kompetencji i funkcji i może ograniczyć efektywność bezpieczeństwa cybernetycznego Wielkiej Brytanii.

Realizacja strategii

W realizacji długoterminowych celów udało się wypracować działania ukierunkowane na zwiększenie współpracy pomiędzy sektorem publicznym i państwowym. Rząd opublikował poradnik o cyberbezpieczeństwie skierowany dla przedstawicieli biznesu. Udało się również zorganizować serię spotkań pomiędzy prywatnymi przedsiębiorstwami i GCHQ, które przyniosły pozytywne efekty. W ramach kooperacji z przedsiębiorstwami odpowiedzialnymi za infrastrukturę krytyczną utworzono program, mający na celu wymianę informacji, zatytułowany „*Sharing Partnership*” (Shah Sooraj). Jednak najważniejszy sukces we współpracy z sektorem prywatnym odnotowano poprzez zawarcie umów o współpracy z największą brytyjską firmą zbrojeniową – BAE Systems i jednym z największych operatorów telefonii komórkowej Vodafone (Chuter). Pozytywnie przebiegają też działania ukierunkowane na wzmocnienie zdolności policji w efektywnym ściganiu cyberprzestępców poprzez powołanie „*Police Central eCrime Unit*”. Osiągnięto też zdecydowane postępy w badaniach nad szybszym wykrywaniem nowych szkodliwych programów oraz zapobieganiu atakom hackerskim w Ministerstwie Spraw Obronnych jak i w GCHQ. Udało się również osiągnąć sukces w budowaniu umiejętności do walki w cyberprzestrzeni poprzez nawiązanie kontaktów z Uniwersytetem w Oksfordzie, gdzie będzie rozwijany program kształcący specjalistów od bezpieczeństwa cybernetycznego. Istotna była też inicjatywa „*The Cyber Security Challenge*”, do której zarejestrowało się ponad 10 tys. osób, duża część z nich zdała testy i znalazła zatrudnienie (Shah Sooraj).

Wielka Brytania odniosła też sukcesy w realizacji swojej strategii na forum międzynarodowym. Podczas spotkania brytyjskiego premiera z prezydentem Stanów Zjednoczonych zawarto umowę o pogłębieniu bilateralnej współpracy pomiędzy krajami w zwalczaniu cyberprzestępczości poprzez m.in. wymianę informacji o cyberatakach oraz zapewnieniu wolności w Internecie. Zapowiedziano też konsultację z Australią odnośnie opracowania placówki badawczej zajmującej się rozwojem zagrożeń w cyberprzestrzeni (Fryer-Biggs, Zachary). Premierowi Cameronowi udało się podpisać porozumienie o bezpieczeństwie cybernetycznym z Indiami, które ma chronić m.in. brytyjskich inwestorów w tym kraju (Kirkup James).

Podsumowanie

Analiza oficjalnych dokumentów brytyjskiej administracji pozwala jednoznacznie stwierdzić, że cyberbezpieczeństwo jest przez Londyn traktowane jak najbardziej poważnie. Pierwsze zapisy dotyczące tego problemu

pojawiły się w 2009, wraz z opublikowaniem strategii bezpieczeństwa narodowego i strategii bezpieczeństwa cybernetycznego. Zapisy te zarysowały szkic tej istotnej kwestii oraz stworzyły fundament do walki z tym zagrożeniem. Jednak, oba dokumenty były krytykowane za zbyt ogólne sformułowania i małą liczbę sugestii jak dany problem rozwiązać. Trzeba jednak wziąć pod uwagę, że w tamtym czasie Wielka Brytania była jednym z pierwszych krajów pracujących nad rozwojem kompleksowej strategii bezpieczeństwa cybernetycznego, a sam dokument miał raczej wyznaczać drogę, a nie tworzyć dokładne rozwiązania. Nowy rząd, który doszedł do władzy potraktował zagrożenie cybernetyczne jako jedno z najpoważniejszych, wdrożył również kompleksową strategię cyberbezpieczeństwa, w którym opisano szczegółowo zagrożenia, jak również zawarto sugestie ich zwalczania w przyszłości. Co więcej, mimo redukcji wydatków na zbrojenia, nakłady na cyberbezpieczeństwo wzrosły. Wydaje się, że obecnie Wielka Brytania posiada znaczące środki obrony w cyberprzestrzeni, oparte na jasnych zapisach w dokumentach strategicznych, które stanowią doskonały fundament do dalszego rozwoju. Co więcej, po roku od wdrożenia strategii, widać, że nie jest ona martwym dokumentem, a jej zapisy są realizowane w praktyce.

Bibliografia

- A Strong Britain in an Age of Uncertainty: The National Security Strategy*. (http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf, dostęp 09.10.2010)
- Chuter, Andrew. "BAE, Vodafone Join in Cybersecurity Partnership". *Defence News*. (<http://www.defensenews.com/article/20130218/DEFREG01/302180012>, dostęp 04.03.2013)
- Cyber Security Challenge UK*. (<https://cybersecuritychallenge.org.uk/competitions.php>, dostęp 15.03.2013)
- Cyber Security Strategy of the United Kingdom. Safety, Security and Resilience in Cyberspace*. UK Cyber Security Operations Centre, June 2009. (<http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf>, dostęp 05.03.2013)
- Florêncio, Dinei, Herley Cormac. "The Cybercrime Wave That Wasn't". *The New York Times*, April 12, 2012, http://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=0, dostęp 25.02.2013)
- Fryer-Biggs, Zachary. *U.K., U.S. Outline Future Cyber Cooperation*, *Defence News*. March 14, 2012. (<http://www.defensenews.com/article/20120314/DEFREG02/303140002/U-K-U-S-Outline-Future-Cyber-Cooperation>, dostęp 04.03.2013)
- Guy, Laurence. *The Internet Economy in the United Kingdom*. AT Kearney, January 01, 2012. (http://www.atkearney.com/en_GB/paper//asset_publisher/dVxv4Hz2h8bS/content/the-internet-economy-in-the-united-kingdom/10192, dostęp 25.02.2013)

- In the Dark. Crucial Industries Confront Cyberattacks*. Center for Strategic Studies, 2011. (<http://www.mcafee.com/us/resources/reports/rp-criticalinfrastructure-protection.pdf>, dostęp 05.03.2013)
- Keeping Our Society Safe and Successful in the Internet Age*. (<http://www.gchq.gov.uk/Pages/homepage.aspx>, dostęp 26.02.2013)
- Kirkup, James. "David Cameron to Strike Cybercrime Deal with India". *The Telegraph*. February 13, 2013. (<http://www.telegraph.co.uk/news/politics/9879272/David-Cameron-to-strike-cybercrime-deal-with-India.html>, dostęp 04.03.2013)
- Korns, W. Stephen, Kastenberga E. Joshua. *Georgia's Cyber Left Hook Parametr.* Office for National Statistics (Winter 2008/2009): 61-76. (<http://www.ons.gov.uk>, dostęp 05.03.2013)
- Phishing – łowienie naiwnych*. CHIP. November 19, 2009. (http://www.chip.pl/artykuly/trendy/2009/11/phishing-lowienie-naiwnych?b_start:int=0, dostęp 25.02.2013)
- Rattray J. Gregory. *Wojna strategiczna w cyberprzestrzeni*. Warszawa: Wydawnictwo Naukowo-Techniczne, 2004.
- Sanger, David. *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power*. Now York: Crown Publishers, 2012.
- Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*. HM Government. October 2010. (http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf, dostęp 05.03.2013)
- Shah, Sooraj. *One Year on: The UK Cyber Security Strategy*. December 3, 2012. (<http://www.computing.co.uk/ctg/news/2229166/one-year-on-the-uk-cyber-security-strategy>, dostęp 04.03.2013)
- Stachowski, Tomasz. *Cyberbezpieczeństwo w nowej strategii bezpieczeństwa narodowego Wielkiej Brytanii*. Metodologia Badań Bezpieczeństwa Narodowego. Bezpieczeństwo 2010, oprac. Piotr Sienkiewicz, Maciej Marszałek, Halina Świeboda.
- The Cost of Cybercrime*, BAE Systems Detica, November 2, 2011. (https://www.baesystemsdetica.com/uploads/press_releases/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf, dostęp 05.03.2013)
- The National Security Strategy of the United Kingdom*. Update 2009. Security of the Next Generation 2009. (<http://www.computerweekly.com/blogs/read-all-about-it/NationalSecurityStrategy2009v2.pdf>, dostęp 05.03.2013)
- The Rough Guide to Online Safety*. 2011. (http://www.getsafeonline.org/themes/site_themes/getsafeonline/pdf/GetSafeOnline_RoughGuide.pdf, dostęp 26.02.2013)
- The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World*. HM Government. November 2011. (<http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf>, dostęp 05.03.2013)
- Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia". *The Guardian*. May 17, 2007. <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>, dostęp 25.03.2013)
- UK Cyber Security Strategy – Even More Bureaucracy, but No Financial Budget. Legislative Power or Democratic Accountability*. January 27, 2009.
- World Internet Users and Population Stats*. Internet World Stats. June 30, 2012, (<http://www.internetworldstats.com/stats.htm>, dostęp 25.02.2013)

Cybersecurity in Strategic Documents of Great Britain 2009-2011

Summary

This essay tries to answer the question about the role and place of cybersecurity in the most crucial strategic documents of Great Britain in the period between 2009 and 2011. Cyberspace plays an important role for the states and their societies and because of this fact setting an efficient strategy in this domain is inevitably crucial. This article presents a comprehensive analysis of national security strategies as well as the cyberstrategies. The most important priorities, the methods and tools of achieving them and the role of the crucial bodies responsible for Great Britain cybersecurity are described. The analysis of the national security strategies allows to highlight the role of the cybersecurity in these documents.