Cyber freedom versus cyber security

Cyberwolność versus cyberbezpieczeństwo

Monika Szyłkowska

Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego w Warszawie
Wydział Logistyki
Katedra Systemów Bezpieczeństwa i Obronności

Abstract

The article presents counterpoints cyber freedom and cybersecurity as determinants of shaping and functioning of the information society and the challenges that imply in the issues of the necessary regulations. In the discussion determinated by the topic, this article presents selected problems and considerations of selected aspects: the idea of freedom of the Network and Network users – awareness of their actions, motives and dangers related with using of the Web, its resources and the simultaneous functioning in a `real` reality – and virtual reality. In turn, the aspect of cybersecurity – in the mainstream discussion of this article – mainly refers to the results of tests conducted in people aged 18-26 years, in particular with regard to: the use of the network and its resources, anonymity and false sense of anonimity in network, knowledge of the rules and regulations about downloading and sharing files.

Streszczenie

Artykuł przedstawia kontrapunkty cyberwolności i cyberbezpieczeństwa jako determinanty kształtowania i funkcjonowania społeczeństwa informacyjnego oraz wyzwania, jakie implikują w zakresie koniecznych

regulacji. W obszarze rozważań zakreślonych tematem, niniejszy artykuł przedstawia część dociekań wybranych problemów w aspektach idei wolności Sieci oraz użytkowników Sieci – świadomości ich działań oraz motywów korzystania z Sieci, jej zasobów oraz funkcjonowania w symultanicznej do realnej płaszczyźnie wirtualnej. Z kolei aspekt cyberbezpieczeństwa – w nurcie rozważań niniejszego artykułu – odnosi się w głównej mierze do wyników badań przeprowadzonych w grupie osób w wieku 18-26 lat, w szczególności w aspekcie korzystania z Sieci i jej zasobów, anonimowości i fałszywego poczucia jej posiadania, znajomości zasad i regulacji dotyczących legalnego pobierania plików oraz ich udostępniania.

Keywords:
Global Network, information society, anonimity, simultaneous reality, the idea of the Network, security in Cyberspace, freedom in Cyberspace

Słowa kluczowe:
Globalna Sieć, społeczeństwo informacyjne, anonimowość, symultaniczna rzeczywistość, idea Sieci, bezpieczeństwo w cyberprzestrzeni, wolność w cyberprzestrzeni

Wprowadzenie

Niniejszy artykuł zawiera rozważania wybranych problemów w zakresie kluczowych determinantów funkcjonowania społeczeństwa informacyjnego: cyberwolności i cyberbezpieczeństwa. Oba słowaklucze zostały użyte jako kontrapunkty. O jednym i drugim zagadnieniu można mówić w różnych płaszczyznach i odniesieniach, ale na potrzeby niniejszej publikacji zostały wybrane najbardziej symptomatyczne z pozycji użytkownika Sieci. Punktem wyjścia rozważań były wyniki badań przeprowadzone na potrzeby rozprawy doktorskiej (*Ochrona cyberprzestrzeni w systemie bezpieczeństwa narodowego Rzeczpospolitej Polskiej*, Szczytno 2014), których część stała się implikacją do poszukiwania odpowiedzi na pytanie: jak wygląda *rzeczywistość świata cyfrowego* młodego pokolenia i dlaczego cyberwolność jest jego kluczowym składnikiem? W artykule ujęto zasadniczy problem

badawczy, w ramach którego wykorzystano podstawowe metody teoretyczne: analizę, analogię oraz wnioskowanie oparte o część wyników badań ankietowych, przeprowadzonych na potrzeby rozprawy doktorskiej autorki.

W literaturze przedmiotu szeroko podejmowano dotąd kwestie w obszarze bezpieczeństwa informacyjnego, społeczeństwa informacyjnego czy cyberbezpieczeństwa w różnych płaszczyznach i poziomach (organizacyjnych, instytucjonalnych). Brakuje natomiast pozycji traktujących o tych kluczowych zagadnieniach z punktu widzenia użytkownika Sieci. W zakresie tematyki związanej z szeroko pojętym bezpieczeństwem informacyjnym, do szczególnie interesujących należą: *Terroryzm w cybernetycznej przestrzeni Profesora Piotra Sienkiewicza,* w (red.) Jemioła T., Kisielnicki J., Rajchel K. *Cyberterroryzm – nowe wyzwania XXI wieku, Bezpieczeństwo informacyjne* K. Lidermana, *Teoria społeczeństwa Sieci* F. Staldera, *Walka informacyjna* L. Ciborowskiego, *Informacyjny wymiar bezpieczeństwa narodowego* K. Liedla, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego* P. Bączka, czy *Prawo karne komputerowe* A. Adamskiego.

Należy również wymienić takie pozycje-klasyki, jak: *Neuromancer* W. Gibsona, *Bomba megabitowa* S. Lema, czy *Limes inferior* A. Zajdla. Poza tym warto wspomnieć: *Wirtualne realis*. *Estetyka w epoce elektroniki* M. Ostrowickiego czy *Rozmowy z cyfrowym cieniem* P. Sitarskiego.

Cyberprzestrzeń

Warto przybliżyć na początku rozważań pojęcie cyberprzestrzeni, ponieważ jest kluczem do zrozumienia idei wolności Sieci i istoty cyberwolności.

Nowy wymiar, określany mianem *cyberprzestrzeni,* zainicjowany został wraz z rewolucją techniczną, a dokładniej z nowoczesnymi rozwiązaniami tak w zakresie sprzętu, jak i oprogramowania. Pojęcie *cyberprzestrzeni* sięga lat 80. XX wieku, kiedy prawdopodobnie po raz pierwszy określenie to zostało użyte przez amerykańskich specjalistów wywiadu wojskowego. Pojęcie to można rozpatrywać w różnych aspektach: technicznym, technologicznym, społecznym, psychologicznym i ekonomicznym. Niezależnie jednak od przyjętej płaszczyzny trudno jednoznacznie odseparować je od siebie, ponieważ, z przyczyn oczywistych, podlegają przenikaniu.

Nazwa źródłowa pojęcia *cyberprzestrzeń* (ang. *cyberspace*) jest związana z cybernetyką, czyli nauką o systemach sterowania oraz przetwarzania i przekazywania informacji (komunikacja, Źródło: http://pl.wikipedia.org/wiki/Cybernetyka). Inne źródła uznają za twórcę tego pojęcia amerykańskiego pisarza, Williama Gibsona, który w swojej powieści *Neuromancer* napisał: *To jest cyberprzestrzeń konsensualna, halucynacja, doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach (…). Graficzne odwzorowanie danych (…) wszystkich komputerów świata. Niewyobrażalna złożoność* [Nowak J., *Cyberprzestrzeń – tam, gdzie nie ma tam].* Najpełniej charakter cyberprzestrzeni oddaje jednak inne zdanie tegoż autora: *cyberprzestrzeń jest królestwem przestrzennych paradoksów, gdzie tam nie ma tam* (Gibson W.: *Neuromancer,* 2009. Cyt. również w: *Cyberprzestrzeń nową sferą walki XXI wieku, http://tadeuszjemiolo.natemat.pl/*).

W ogólnym ujęciu cyberprzestrzeń to obszar wirtualny, nieograniczony czasem i przestrzenią, *domeną bitów – uporządkowanych matematycznie poprzez kod binarny abstrakcyjnych form rzeczywistości* (M. Konieczniak, *Poszukiwanie tożsamości w cyberprzestrzeni. Implikacje pedagogiczne*).

Cyberprzestrzeń może być zatem rozumiana jako przestrzeń komunikacyjna, w której występuje wymiana oraz sprzężenie zwrotne – przesyłanie, przetwarzanie i interpretacja informacji. Tak pojmowana cyberprzestrzeń jest wirtualną przestrzenią cyfrowej infosfery. W potocznym znaczeniu cyberprzestrzeń rozumiana jest często jako rzeczywistość wirtualna (w myśl angielskiej definicji słowo: *wirtualny* – oznacza: *symulujący coś, co w istocie nie istnieje, New Hackers Dictionary*). Sitarski konstatuje: *wirtualna rzeczywistość posiada wszystkie cechy prawdziwego świata, oprócz jednej – istnienia* (Sitarski P., *Rozmowy z cyfrowym cieniem*, 2002). Nieposiadająca istnienia wirtualność jest bardzo rzeczywista i pomimo braku fizycznego istnienia silnie odciska swój wpływ na rzeczywistość, ponieważ człowiek coraz bardziej przenosi swoje życie do cyberprzestrzeni (E. Bendyk, *Antymatrix. Człowiek w labiryncie Sieci*, 2004, s. 17). W efekcie realność i wirtualność przenikają się wzajemnie, zacierając i tak dość płynne granice. Według Wolfganga Welsch`a: *wirtualność także bywa realna, kiedy wstępujemy w świat wirtualny, jak w realny* (…), zatem a contrario (…): możemy przypuścić*, że wszystko realne z innego punktu widzenia – jest wirtualne* (M. Ostrowicki: *Wirtualne realis*. *Estetyka w epoce elektroniki*, 2006, s. 32).

Słownik PWN wyraz *wirtualny* definiuje dwojako: 1. *wykreowany na ekranie komputera, telewizora, ale tak realistyczny, że wydaje się rzeczywisty,* 2. *stworzony w ludzkim umyśle, ale prawdopodobnie istniejący w rzeczywistości lub mogący zaistnieć* (Portal internetowy PWN: Słownik Języka Polskiego, http://sjp.pwn.pl/). Tak rozumianą potocznie wirtualność można stosować naprzemiennie z cyberprzestrzenią.

Cyberprzestrzeń stanowi obszar prowadzący z jednej strony do rozwoju, w szczególności w sferze społecznej (komunikacja, edukacja, gospodarka, bezpieczeństwo powszechnego, itp.), z drugiej zaś – generujące zagrożenia takie, jak np.: cyberprzestępczość, cyberinwigilacjia cyberterroryzm czy cyberwojny (P. Sienkiewicz *Terroryzm w cybernetycznej przestrzeni)*.

Reasumując, można przyjąć, że cyberprzestrzeń jest to taki obszar (Sieci zewnętrzne, Sieci wewnętrzne, komputery, systemy), w którym funkcjonuje zdigitalizowana informacja wytworzona przez człowieka (twórcę informacji) w dowolnej formie (dźwięk, obraz, itp.). W obszarze tym informacja może być wytwarzana, przetwarzana, transmitowana i przechowywana, determinując dalsze powiązania i działania poprzez cele (cel powstania) i funkcje (przekazanie informacji), aby osiągnąć za jej pomocą określony skutek (szerzej w: Rozprawa doktorska: *Ochrona cyberprzestrzeni w systemie bezpieczeństwa narodowego Rzeczpospolitej Polskiej.* Szczytno, 2014).

Cyberwolność

Cyfrowa rewolucja przyniosła *rzeczywistość przyszłości* opisywaną wcześniej przez autorów science-fiction (Gibson, Lem, Zajdel, Lukas) i porywającą odbiorców do snucia marzeń o nadejściu takiej przyszłości. Urzeczywistnienie tych śmiałych wizji (możliwości porozumiewania się na odległość czy stworzenia wirtualnej rzeczywistości) zapoczątkowała dostępność Internetu dla wszystkich wraz z przełomowym wynalazkiem Tima Berners`a – Lee w postaci World Wide Web (opracowanie przez naukowców z CERN standardu www datowane jest na rok 1991) oraz podstaw HTML. Globalna Sieć, którą znamy obecnie, zawdzięcza swoje powstanie realizacji marzenia jej twórców o urzeczywistnieniu idei równości i wolności tak w dostępie, jak i możliwości czerpania z jej zasobów. Początek dzisiejszego *kształtu* Sieci sięga

lat 70. XX wieku, kiedy to rozkwitła w Stanach Zjednoczonych kontrkultura z prądem filozoficznym, zwanym libertarianizmem, odrzucającym kontrolę państwa, system prawny i cenzurę, podkreślającym znaczenie wolnej woli jednostki. Mimo że ówczesne ideały nie wytrzymały zderzenia z realnym światem, to rozkwitły w Sieci, przejmując jej wartości, strukturę oraz niechęć do szeroko rozumianej kontroli i władzy. Za pierwszą *wirtualną społeczność* (prawdopodobnie jako pierwszy użył tego sformułowania Howard Rheingold), czy też *ruch społeczny*,uznawane jest The WELL™ (*miejsce, które znajduje się kilka klawiszy klawiatury stąd, niezależnie od tego, gdzie jesteś*). Najbardziej znany jej członek napisał *The Whole Earth Catalogue* uznawaną za *Biblię kontrkultury*. Przyjmuje się, że *Studnia* (ang. well) zdefiniowała dzisiejszą postać Sieci, kiedy w czasie jej początków dostęp do Internetu miało zaledwie 1% mieszkańców Ziemi (źródło: *Wirtualna Rewolucja*, BBC 2010). Stewart Brand, twórca The WELL™: *Chcieliśmy stworzyć przestrzeń, w której moglibyśmy realizować własne pomysły, eksperymentować. Nie mieliśmy wówczas pieniędzy ani wpływów, ale zdawaliśmy sobie sprawę z szansy, jaka się przed nami pojawiła* (źródło: wywiad dla dr Aleks Krotoski, *Wirtualna Rewolucja*, BBC 2010) (…) *Każdy mógł tam powiedzieć wszystko. Nikt nikogo nie oceniał ani nie krytykował*. Kolejną ikoną The WELL jest znany amerykański poeta, eseista, John Perry Barlow, który przedstawił cyberprzestrzeń w niezwykle obrazowy sposób, trafnie porównując ją w obecnym kształcie do XIX-wiecznego *Dzikiego Zachodu* – Pogranicza. Oba obszary łączy to, że stanowią nieopisane, rozległe terytorium, niejednoznaczne kulturowo i prawnie, co z jednej strony powoduje trudności w poruszaniu się, z drugiej zaś jest otwarte na zasiedlanie. Barlow określa również cyberprzestrzeń jako *dom umysłu /cywilizację umysłu*. Idea nieograniczonej wolności słowa Barlowa rozbija się jednak o dzisiejszą rzeczywistość wirtualnych zagrożeń, których realne skutki kończą się czasem tragicznie, np. falą tzw. hejtu, uświadamiając, że nie wszyscy użytkownicy mają dobre intencje. W imię idei równych szans należy pomyśleć o tych słabszych i często nieświadomych skali i rodzajów zagrożeń. Natomiast tragiczne w skutkach zdarzenia wpływają na dyskusję o konieczności wprowadzenia regulacji w tym zakresie.

Gibsonowski paradoks przestrzenny świata wirtualnego – gdzie *tam nie ma tam* – implikuje poszukiwanie odpowiedzi na pytania: jak wygląda dzisiejszy świat i rzeczywistość użytkowników Sieci? Z pewnością jest

ona dualna i symultaniczna. W zależności od wyboru można dzisiaj żyć w jednym, pomiędzy lub w *dwóch światach* jednocześnie. Użytkownik Sieci ma możliwość utrzymywania kontaktów z osobami oddalonymi o tysiące kilometrów w czasie rzeczywistym bez konieczności wychodzenia z domu. W świecie cyfrowym, tak jak *analogowym,* musi jednak się odnaleźć, nadać sobie tożsamość i wyrazić siebie, np. poprzez profile w portalach społecznościowych, blogach czy na forach. Nie jest już nowym odkryciem, że człowiek przenosi tradycyjne potrzeby i pragnienia do świata wirtualnego, szuka podobnych do siebie pod względem wyznawanych wartości, zainteresowań czy hobby. Wymienia się poglądami, wspiera, czerpie z cyfrowych źródeł kultury, nauki, rozrywki – ze wszystkich dostępnych w Sieci miejsc w różnych formach. Spostrzeżenie to *dotyka* **istoty cyberwolności, jako możliwości wyrażania siebie w dowolny sposób, w dowolnej formie, w dowolnym czasie i miejscu cyfrowego świata** (np. poprzez określone przez siebie profile, fora dyskusyjne, zdjęcia czy filmy) **oraz jako możliwości korzystania z nieograniczonych zasobów informacji** według własnych potrzeb i upodobań, w dowolnym czasie, **bez cenzury, bez kontroli, bez nadzoru, *bez paszportu* i czyjejkolwiek zgody,** odpowiedzialnie lub nie.

Cyberwolność to potężna siła i dlatego użytkownicy powinni umieć z niej korzystać. Jak w każdym wymiarze, człowiek ze swoimi nawykami, skłonnościami i nierzadko ułomnościami może wykorzystać każde narzędzie w sposób pozytywny i konstruktywny lub negatywny i destrukcyjny. Może krzywdzić lub pomagać. W świecie *analogowym* istnieją określone zasady, regulacje, normy społeczne w skali makro i mikro. Na co dzień ludzi determinują role, obowiązki, wybrane zawody. Z częścią się zgadzają, innych woleliby nie mieć, ale przyjmują je niejako *a priori*. Granice wolności osobistej wyznacza tak naprawdę wolność innych – w myśl słów A. de Tocqueville`a: *Wolność człowieka kończy się tam, gdzie zaczyna się wolność drugiego człowieka*. W niektórych gałęziach prawa przyjęta jest zasada, która głosi, że co nie jest zabronione, jest dozwolone, a mimo to jednostki nie korzystają z przesadą ze swoich swobód dla dobra ogółu. Wydawałoby się, że jest to oczywiste i normalne. Jednak, *zaglądając* do świata cyfrowego, można dostrzec, że porównywanie go do *Dzikiego Zachodu* ma swoje głębokie uzasadnienie. Wystarczy przeczytać komentarze dowolnego artykułu w dowolnym portalu informacyjnym, aby

zobaczyć upust nienawiści, który kilka linijek niżej nie dotyczy już nawet komentowanego artykułu, tylko staje się polem bitwy na personalne, chociaż nieznanych sobie osób, wojny. Użytkownicy takich postów za zasłoną *nicków* czują się anonimowi i bezkarni. Kształtuje się tym samym cyfrowa wolność *od* i *do* – wolność do działania i wyrażania siebie oraz korzystania z zasobów Sieci, ale i wolność od zagrożeń czy ograniczania swobody.

Fikcyjne poczucie anonimowości

Użytkownicy nieobeznani z technicznymi aspektami Sieci przeważnie nie zdają sobie sprawy z faktu, że IP (Internet Protocol) ich urządzeń jest jak numer rejestracyjny samochodu lub adres zamieszkania. Paradoksem jest również fakt, że chcieliby zachować pełną anonimowość, ale większość z nich bez dłuższej refleksji umieszcza swoje zdjęcia na portalach społecznościowych, z obfitującymi w szczegóły informacjami o sobie.

Dla badanych użytkowników Sieci istota cyberwolności wyraża się także możliwością darmowego pobierania plików, ale w pytaniu ankietowym, dotyczącym znajomości przepisów i zasad dotyczących legalnego pobierania, większość przeczyła posiadaniu wiedzy w tym zakresie. Co do zasady obywatele często są przeciwni ograniczeniom na rzecz bezpieczeństwa, jednocześnie nie będąc świadomi faktu, że wszelka *prywatna* działalność w cyberprzestrzeni nie jest *niewidzialna* i anonimowa – poza wspomnianym wyżej IP. Każdy wpis na forum, zrobienie zakupów, zapłacenie rachunków czy zarezerwowanie biletu tworzą swoisty cyberprofil, który jest cennym zbiorem przede wszystkim dla prywatnych firm, oferujących swoje usługi również, a może przede wszystkim, w Sieci. Profil ten pomaga personalizować ofertę dopasowaną później do określonych preferencji, sporządzonych właśnie dzięki przeanalizowanym zachowaniom użytkowników. W związku z tym uświadomienie użytkowników w wyżej wskazanym zakresie, z dużą dozą prawdopodobieństwa zmieniłoby ich stosunek do zmian w sferze przetwarzania informacji na poziomie państwowym, w tym propozycjom regulacji w tym zakresie.

Warto podkreślić, że obecnie istnieje już możliwość precyzyjnego zidentyfikowania urządzenia zasilanego baterią (np. tabletu, notebooka, czy smartfonu) na podstawie jego akumulatora (sic!) niezależnie od adresu IP.

Cyberzagrożenia

Tytułem wprowadzenia w istotę i zakres cyberbezpieczeństwa warto syntetycznie przedstawić klasyfikację cyfrowych zagrożeń. Podstawowe grupy zagrożeń to zagrożenia:

- wynikające z działalności człowieka, w tym: celowe (cyberprzestępcy, cyberterroryści, *pozawirtualni* przestępcy, np. kradzież lub uszkodzenie urządzeń) i niecelowe (nieprzeszkoleni pracownicy);
- wyni*kające z natu*ralnego środowiska (katastrofa naturalna, powodująca np. brak zasilania);
- niezwiązane z celową działalnością człowieka (zawodność systemów, błędy w oprogramowaniu, awarie zasilania).

Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów KOM(2007) 267 [22 maja 2007 r.], dotyczący ogólnej strategii zwalczania cyberprzestępczości, sklasyfikował przestępstwa w cyberprzestrzeni w trzy podstawowe rodzaje, a mianowicie w:

- **tradycyjne formy**, tj. oszustwo i fałszerstwo z wykorzystaniem elektronicznych Sieci informatycznych oraz systemów informatycznych (sieci łączności elektronicznej). Do najczęstszych z nich należą oszustwa na masową skalę za pomocą takich metod, jak: kradzież tożsamości, spam, robaki i wirusy, *phishing* oraz nielegalny handel na skalę międzynarodową (narkotyki, broń, ginące gatunki zwierząt);
- **p*ublikacj*e nielegalnych treści w mediach elektronicznych, a w tym:** strony internetowe zawierające nielegalne treści, takie jak: nawoływanie do nienawiści rasowej, podżeganie do aktów terrorystycznych itp. Przestępstwa tego rodzaju są trudne do ścigania, przede wszystkim z uwagi na fakt, iż właściciele i administratorzy stron niejednokrotnie są obywatelami innych krajów, najczęściej spoza UE, gdzie definicje nielegalnych treści są różne. Poza tym przeniesienie treści strony na serwer innego kraju jest łatwe i może nastąpić w ciągu kilkunastu minut;
- **przestępstwa „typowe" dla Sieci**, tj.: ataki hakerskie, przeciwko systemom informatycznym, ataki typu DDoS. Ataki tego typu

> mogą być również skierowane przeciwko infrastrukturom krytycznym państw europejskich, stanowiąc relatywnie największe zagrożenie ze względu na potencjalnie dramatyczne konsekwencje dla całego społeczeństwa. Nie bez znaczenia pozostaje fakt łączenia technologii i tworzenia powiązań pomiędzy systemami informatycznymi, co w konsekwencji ułatwia podatność na ataki tego typu. Najczęstszym celem ataków jest wymuszenie *okupu* ze względu na potencjalne straty, jakie mogłyby przynieść przedsiębiorstwom, gdyby została upubliczniona informacja o problemach z zapewnieniem bezpieczeństwa.

Dla prywatnych użytkowników największe zagrożenie stanowią obecnie luki w zabezpieczeniach urządzeń mobilnych, takich jak smartfony czy tablety. Według danych udostępnionych przez firmy specjalizujące się w oprogramowaniu zabezpieczającym, w Sieci krąży ok. 865 000 wirusów, atakujących tego rodzaju urządzenia. Znamienny przykład może stanowić możliwość odczytania zapisanego w systemie jednego z rodzajów telefonów (znanego producenta) odcisku palca zapisywanego w systemie urządzenia, służącego do logowania i zabezpieczania (sic!). Z uwagi na fakt, że linie papilarne są niepowtarzalne, niezabezpieczony plik graficzny z danymi biometrycznymi stanowi ogromne zagrożenie z dwóch powodów: poza możliwością przejęcia kontroli nad danym urządzeniem, dane takie mogą posłużyć do kradzieży tożsamości użytkownika (źródło: J. Gozdek, *Hakerzy bez granic*, CHIP 11/2015, s. 105).

Cyberbezpieczeństwo

Kontrapunktem w niniejszym artykule dla cyberwolności jest cyberbezpieczeństwo. Z przeprowadzonych badań w grupie osób w wieku 18-26 lat jeden z kluczowych wniosków stanowi, że młodzi ludzie *chcą mieć wszystko* – nie chcą kontroli, chcą zachować anonimowość i posiadać szeroko rozumianą wolność w Sieci, ale jednocześnie chcą *być* bezpieczni i *czuć się* bezpiecznie, a tego rodzaju bezpieczeństwo, zdaniem badanych, powinny zapewnić instytucje państwowe, np. poprzez darmowe, *rządowe* programy antywirusowe oraz instytucję, która informowałaby o zagrożeniach i sposobach ich

minimalizowania. Na pytanie o wyrażenie zgody na wprowadzenie ograniczeń w dostępie do treści zawartych w Sieci z uwagi na własne bezpieczeństwo, 42% zakwestionowałoby tego rodzaju propozycję, 31% byłoby skłonnych zgodzić się na taką możliwość w wyjątkowych przypadkach, natomiast 14% wyraziłoby zgodę bez dodatkowych warunków (rys.1-3). Z kolei na pytanie: czy treści godzące w podstawowe wartości lub zagrażające bezpieczeństwu powinny być usuwane z Sieci lub dostęp do nich powinien być uniemożliwiony, aż 42% zgodziło się z takim działaniem, 17% było zdania przeciwnego, zaś 28% nie miało zdania na ten temat (rys. 4). Kolejne pytanie dotyczyło wprowadzenia dodatkowego przedmiotu obowiązkowego z bezpieczeństwa cyberprzestrzeni. Połowa respondentów uznała takie działanie za słuszne, pozostali uznali za właściwe jedynie wprowadzenie tej tematyki do przedmiotu informatyka.

W zakresie znajomości przepisów prawa regulujących możliwość pobierania plików z Sieci, ponad połowa ankietowanych przyznała, że nie posiada takiej wiedzy. Z kolei fakt udostępniania przez respondentów swoich plików w Sieci potwierdziło aż 66% (rys. 5 i 6). Wynikają z tego dwa dodatkowe wnioski: po pierwsze – część internautów nie ma świadomości, że może łamać lub łamie istniejące regulacje, po drugie – grupa ta nie uważa, że tego rodzaju czynności są nielegalne. Oznacza to także, że internauci, nawet jeśli trafiają na strony informujące o nielegalnym pobieraniu plików**,** nie zaznajamiają się z ich treścią.

Kluczowe i najbardziej interesujące wyniki dotyczyły kwestii ściśle powiązanych z cyberbezpieczeństwem, a mianowicie:

- na pytanie dotyczące wpływu cyberprzestrzeni na życie respondentów i sposób ich funkcjonowania, aż 71% badanych uznało, że wirtualna przestrzeń posiada taki wpływ (rys. 7);
- ponad połowa ankietowanych potwierdziła, że istnieje możliwość powstania konfliktu pomiędzy państwami, którego początek będzie w cyberprzestrzeni;
- na pytanie, czy cyberatak może spowodować zagrożenie w funkcjonowaniu państwa, aż 86% respondentów uznało, że jest to możliwe;
- ponad połowa respondentów wyraziłaby zgodę na wprowadzenie kontroli w cyberprzestrzeni w celu zwiększenia poziomu

bezpieczeństwa dla użytkowników, niewiążącą się jednocześnie z żadnym ograniczeniem w zakresie korzystania z Sieci (rys. 8);
- na pytanie: czy respondenci korzystaliby z darmowego oprogramowania zwiększającego bezpieczeństwo w cyberprzestrzeni, pochodzącego od instytucji państwowej, 42% udzieliło twierdzącej odpowiedzi, 9% zdecydowanie tak, ze względu na większe zaufanie do instytucji państwowych w tym zakresie (rys. 9).

Niezwykle interesującym punktem badania było wskazanie przez ankietowanych propozycji, mających na celu poprawienie własnego bezpieczeństwa w Sieci. Do najczęstszych wymienianych należało:
- szyfrowanie danych osobowych;
- darmowy, *rządowy* program ochronny obowiązujący w całym kraju;
- zapewnienie anonimowości użytkowników;
- brak rejestracji w przypadku, gdy należy podać szczegółowe dane, np. nr konta bankowego;
- brak konieczności podawania szczegółowych danych;
- wprowadzenie sensownych ograniczeń;
- zaostrzenie kar za *hakerstwo* i *spam*;
- cenzura;
- nadzór programowy na stronach internetowych;
- lokalizowanie i usuwanie zawirusowanych stron;
- ostrzeżenia przed zagrożeniem;
- powszechnie dostępne szkolenia dotyczące bezpieczeństwa sieciowego;
- powołanie organizacji mającej na celu zapewnienie bezpieczeństwa i kontrolę w Sieci;
- rejestracja adresów IP.

Z technicznego punktu widzenia potencjalne i realne możliwości zapewnienia ochrony cyberprzestrzeni składają się z kilku poziomów: na poziomie podstawowym będzie to świadomość każdego użytkownika cyberprzestrzeni i jego zachowania**,** redukujące lub minimalizujące zagrożenia, szczególnie w sferze prywatnej; na poziomie zaawansowanym będą to działania i zachowania użytkowników, specjalizujących się przede wszystkim w zapewnieniu funkcjonowania Sieci, np. administratorzy, zaś na poziomie

profesjonalnym – osoby odpowiedzialne za bezpieczeństwo Sieci i urządzeń teleinformatycznych. W szerszym odniesieniu, w celu zapewnienia cyberbezpieczeństwa, niezbędne są odpowiednie polityki i strategie bezpieczeństwa oraz poszczególne programy ochrony w tym zakresie, również zróżnicowane pod względem poziomu zaawansowania i szczegółowości.

Ochrona jest podstawą zapewnienia bezpieczeństwa w każdej dziedzinie. Fundament stanowi wiedza i świadomość użytkowników, ponieważ to *czynnik ludzki* odgrywa najważniejszą rolę, stanowiąc zarazem najmocniejsze i najsłabsze ogniwo w łańcuchu bezpieczeństwa. Z kolei odpowiedniej rangi dokumenty są istotne z punktu widzenia organizacji bezpieczeństwa. Zasadniczą kwestią pozostaje jednak edukacja. Wynika to z prostej przyczyny – obecnie każdy może nabyć nowoczesne urządzenie i posługiwać się nim w dowolnych celach. Znajomość podstawowej obsługi w przypadku komputera nie jest jednak jednoznaczna ze świadomością zagrożeń, jakie za sobą niesie, w tym brak chociażby minimalnych sprzętowych czy programowych zabezpieczeń. Z drugiej strony, *zwykły* użytkownik może stać się źródłem realnego zagrożenia, jeżeli na przykład skorzysta z dostępnych w Sieci niebezpiecznych narzędzi, takich jak np. generatory wirusów, i umieści jeden z nich w swoim służbowym komputerze (szerzej w: Rozprawa doktorska: *Ochrona cyberprzestrzeni w systemie bezpieczeństwa narodowego Rzeczpospolitej Polskiej*. Szczytno, 2014).

Podsumowanie

Nie podlega dyskusji fakt, że Sieć zmieniła i wyrównała szanse użytkowników wobec prawa, zasad i możliwości jednakowego, nieograniczonego dostępu do jej zasobów: informacji, wiedzy, kultury i rozrywki oraz prawa głosu do swobodnego wyrażania swoich opinii i dzielenia się wiedzą. *Sieć daje władzę zwykłym ludziom*, stając się *najpotężniejszym narzędziem, jakie kiedykolwiek wynalazł człowiek* (Al Gore w: *Wirtualna Rewolucja*, BBC, 2010).

Cyberwolność stanowi dla użytkowników Sieci warunek *sine qua non* i fundament ich funkcjonowania w *cyfrowym świecie*, który przejawia się zarówno w możliwości wyrażania siebie w dowolnej formie, jak i nieogra-

niczonego korzystania z dostępnych zasobów infosfery. Mimo różnic w poziomie świadomości w zakresie cyfrowych zagrożeń, cyberbezpieczeństwo stanowi dla użytkowników równie ważny czynnik, jednak preferowaliby oni nadzór instytucjonalny.

Reasumując rozważania zakreślone tematem, można sparafrazować klasyczne już powiedzenie konstatacją: *Edukacja, edukacja i jeszcze raz regulacje*. Jednak nie dla ograniczania cyberwolności, ale w jej obronie, aby nie doprowadzić do sytuacji, w której idea początków Sieci: wolności i równego dostępu wszystkich użytkowników do nieograniczonego zasobu informacji, swobody komunikacji i możliwości wyrażania siebie, nie zostanie unicestwiona przez cyfrowy *Dziki Zachód* lub w niedalekiej przyszłości wykorzystana do dyktowania warunków przez największych graczy z sektora prywatnego. Sami użytkownicy mogliby aktywnie uczestniczyć w tworzeniu zasad i praw do Sieci tak, jak ma to obecnie miejsce na przykład w przypadku propozycji włączenia zapisu o *prawie do cyfrowego uczestnictwa* do Karty Praw Podstawowych Unii Europejskiej [(2010/C 83/02)]oraz regulacji zasady neutralności Sieci. Jednak, żeby móc poszukiwać właściwych rozwiązań regulacyjnych, trzeba posiadać wiedzę oraz być świadomym zarówno w zakresie istniejących i potencjalnych zagrożeń, jak i sensownych granic, które można wytyczyć. Dopiero wówczas byłaby to prawdziwa realizacja idei cyberwolności dla cyberbezpieczeństwa, a nie w opozycji do niego.

References

BIBLIOGRAFIA

Bączek, P. (2005). *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*. Toruń: Wyd. Adam Marszałek,.

Barlow, J.P. *Cyberspace Independence Declaration* https://projects.eff.org/~barlow/Declaration-Final.html. Data. dostępu: 10.10.2015 r.

Bendyk, E. (2004). *Antymatrix. Człowiek w labiryncie Sieci*. Warszawa: Wyd. W.A.B.

Dr Krotoski, A. (2010). *Wirtualna Rewolucja*. BBC.

Gibson, W. (1996). *Neuromancer*. Warszawa: Zysk i S-ka,.

Jordan, T. (2011). *Hakerstwo*. Warszawa: Wydawnictwo Naukowe PWN.

Judt, T. (2013). *Brzemię odpowiedzialności. Blum, Camus, Aron i francuski wiek dwudziesty*, tłum. Michał Filipczuk. Warszawa: Wyd. Krytyki Politycznej.

Konieczniak, M. *Poszukiwanie tożsamości w cyberprzestrzeni. Implikacje pedagogiczne*. http://www.ktime.up.krakow.pl/symp2011/referaty2011/konieczniak.pdf. Data. dostępu: 10.10.2015 r.

Magazyn CHIP 11/2015.

New Hackers Dictionary, 2011. http://www.outpost9.com/reference/jargon/jargon_toc.html. Data dostępu: 10.10.2015 r.

Ostrowicki, M. (2006). *Wirtualne realis*. *Estetyka w epoce elektroniki*. Kraków: Universitas.

Pozostałe źródła:

Sienkiewicz, P. (2009). *Terroryzm w cybernetycznej przestrzeni*. W (red.) Jemioła T., Kisielnicki J., Rajchel K.: Cyberterroryzm – nowe wyzwania XXI wieku. Red. Warszawa: Wyższa Szkoła Informatyki, Zarządzania i Administracji.

Sitarski, P.(2002). *Rozmowy z cyfrowym cieniem*. Kraków: Wyd. RABID.

*Słownik PWN: Słownik języka polskiego, http:sjp.pwn.pl.*Data ost. dostępu: 10.10.2015 r.

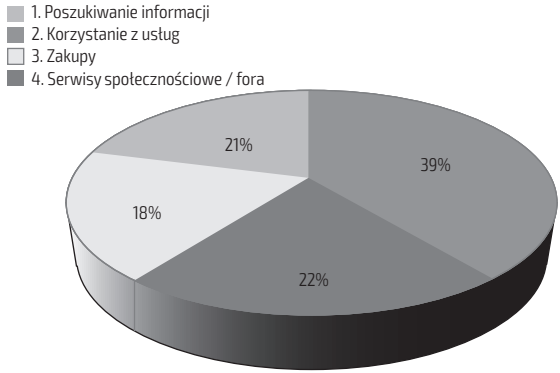
Stadler, F. (2012). *Manuel Castells: Teoria społeczeństwa Sieci*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego,.

The WELL™. http//: www.well.com

Zajdel, J. A. (2010). *Limes inferior*. Wyd. SuperNova [Audiobook].

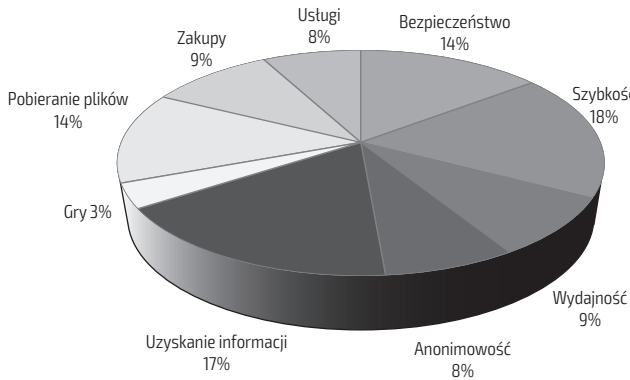
Materiały ilustrujące

Rys.1. Korzystanie z Sieci Internet



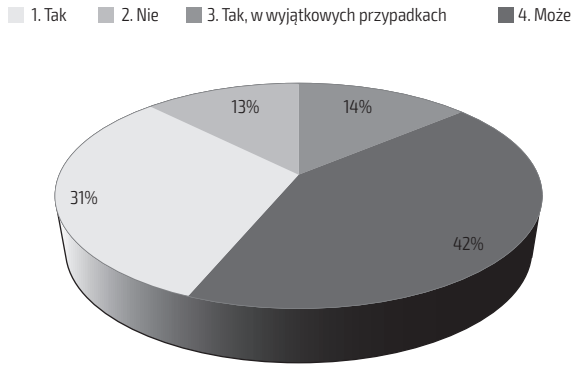
Źródło: opracowanie własne: część wyników badań przeprowadzonych na potrzeby rozprawy doktorskiej autorki: Ochrona cyberprzestrzeni w systemie bezpieczeństwa narodowego Rzeczpospolitej Polskiej. Szczytno, 2014.

Rys. 2. Kluczowe czynniki determinujące poruszanie się w cyberprzestrzeni.



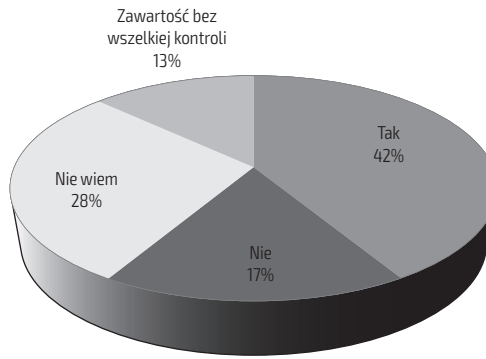
Źródło: opracowanie własne.

Rys. 3. Ograniczenia w dostępie do treści



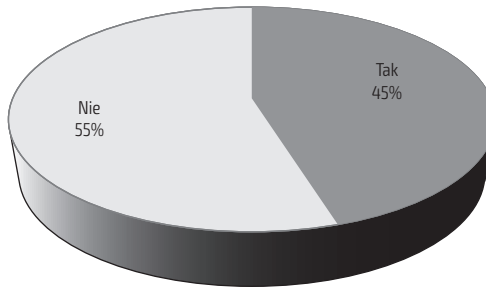
Źródło: opracowanie własne.

Rys. 4. Treści godzące w wartości



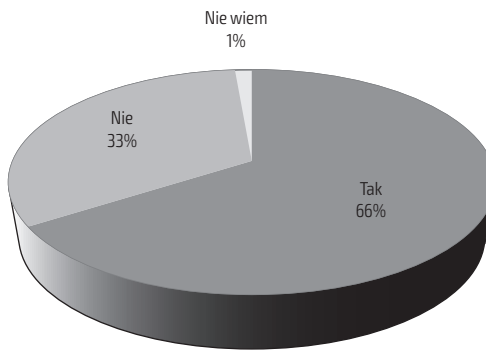
Źródło: opracowanie własne.

Rys. 5. Znajomość przepisów dotyczących pobierania plików



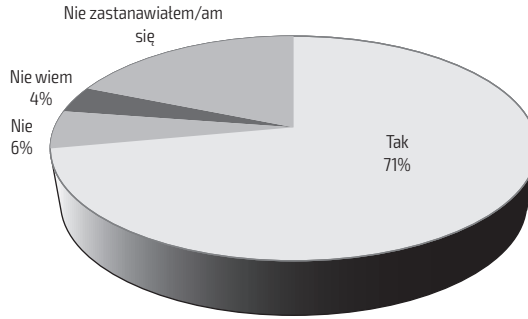
Źródło: opracowanie własne.

Rys. 6. Udostępnianie plików w Sieci



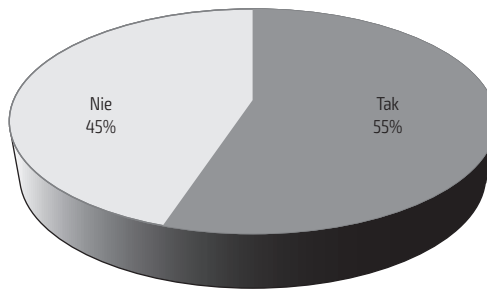
Źródło: opracowanie własne.

Rys. 7. Wpływ cyberprzestrzeni na życie i funkcjonowanie użytkowników



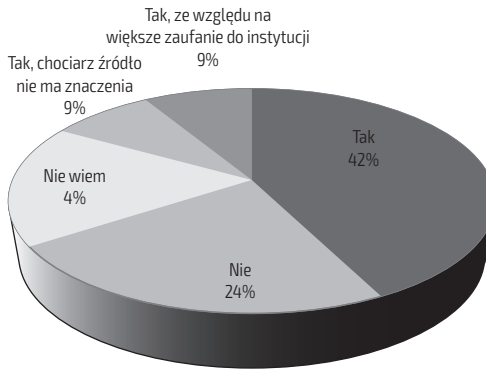
Źródło: opracowanie własne.

Rys. 8. Zgoda na wprowadzenie kontroli



Źródło: opracowanie własne.

Rys. 9. Korzystanie z darmowego oprogramowania zwiększającego bezpieczeństwo w Sieci, pochodzącego od instytucji państwowej



Źródło: opracowanie własne.