Krzysztof Krassowski
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide De Gasperi w Józefowie
kk@wsge.edu.pl

DOI: 10.13166/JMS/92281
JOURNAL OF MODERN SCIENCE TOM 2/37/2018, S. 327–340

A CONCEPT OF INFORMATION AND EDUCATION OF A HUMAN AS TOOL OF PREVENTION OF CYBERSPACE THREATS

KONCEPCJA INFORMOWANIA I EDUKACJI CZŁOWIEKA JAKO NARZĘDZIE PRZECIWDZIAŁANIA ZAGROŻENIOM W CYBERPRZESTRZENI

Abstract

Development of information society of XXI century brought, apart from many welcomed and positive consequences contributing to further development of civilization, also new and unknown threats that are now permanent element of our social reality. Said threats, that are also a subject of constant evolution coupled with advancements of technology, can be characterized by high dynamics of growth and serious negative consequences both regarding high scale material losses they cause as well as other unwanted consequences regarding functioning of whole societies. An efficient countermeasures and fight with the threats in question poses a real challenge to law enforcement and other state institutions responsible for provision and maintenance of public security. Taking into account an economical dimension of discussed phenomenon it seems to be also a field of possible cooperation between public institutions and private sector, vitally interested in minimization of financial loses. Effective neutralization of negative phenomena in cyberspace considered from the point of view of social sciences – taking an education of a human (cyberspace user) as the main point of interest – requires, considering methodology of social sciences, an application of descriptive method for an overview and organization of basic definitions and concepts, together with analysis of phenomenon in question, it's evolution and assessment of strategic countermeasure programs. All this in order to apply a method of synthesis to make determination regarding established issue –

development of both an optimal and practical concept of provision of information and education to a human as an effective means of prevention against cyber threats, in the framework of development of cyberspace culture.

Streszczenie

Rozwój społeczeństwa informacyjnego XXI w. przyniósł, obok wielu pożądanych i pozytywnych skutków korzystnie wpływających na rozwój cywilizacyjny, także nowe, nieznane dotąd zagrożenia, które stały się trwałym elementem naszej rzeczywistości społecznej. Zagrożenia te, same podlegające ciągłej ewolucji wraz z postępującym rozwojem technologii, charakteryzują się dużą dynamiką wzrostu oraz poważnymi negatywnymi konsekwencjami w postaci strat o charakterze materialnym oraz innych niepożądanych skutków dotyczących funkcjonowania całych społeczeństw. Skuteczne przeciwdziałanie i zwalczanie powyższych zagrożeń jest rzeczywistym wyzwaniem dla organów ścigania oraz innych instytucji państwa odpowiedzialnych za zapewnianie bezpieczeństwa publicznego. Ze względu na ekonomiczny wymiar zjawiska jest to również pole ścisłej współpracy instytucji publicznych i sektora prywatnego, żywotnie zainteresowanego minimalizacją strat finansowych. Skuteczna neutralizacja negatywnych zjawisk w cyberprzestrzeni rozpatrywana na gruncie nauk społecznych – przy założeniu, iż edukację człowieka traktuje się jako główny przedmiot zainteresowania – wymaga, z punktu widzenia metodologii nauk społecznych, dla dokonania przeglądu przedmiotowej problematyki i uporządkowania sfery pojęciowej, zastosowania metody opisowej, w połączeniu z metodą analizy zjawiska oraz jego ewolucji i wskazania podejmowanych do tej pory programów zaradczych o charakterze strategicznym. Wszystko to w celu zastosowania metody syntezy dla rozstrzygnięcia w zakresie postawionego problemu – stworzenia praktycznej koncepcji zapewnienia człowiekowi informacji oraz edukacji jako skutecznych narzędzi przeciwdziałania zagrożeniom w cyberprzestrzeni.

Keywords: *cyberspace security, cybercrime, cyberspace threats, information, education*

Słowa kluczowe: *bezpieczeństwo cyberprzestrzeni, cyberprzestępstwo, zagrożenia cyberprzestrzeni, informacja, edukacja*

Wprowadzenie

Rewolucja informacyjna, której świadkami jesteśmy już od kilku dekad, zaowocowała rozwojem nowego typu społeczeństwa, określanego powszechnie jako społeczeństwo informacyjne lub społeczeństwo oparte na wiedzy (Chmura, 2016, s. 301–315). Samo pojęcie społeczeństwa informacyjnego jest

pochodzącą jeszcze z 1963 r. propozycją Tadeo Umesao. Dokonując przeglądu ujęć oraz prób definicji tego pojęcia, wypada zgodzić się z M. Golką, który zauważył, że większość z nich wskazuje na tworzenie, gromadzenie oraz obieg informacji jako warunki niezbędne do funkcjonowania społeczeństwa informacyjnego, zaś sieć (Internet), techniki cyfrowe oraz urządzenia dostępowe (np. komputer) stają się coraz ważniejszym – jeżeli aktualnie już nie najważniejszym – aspektem zarówno pracy, jak i całego życia. Informacja staje się więc najważniejszym, dominującym składnikiem życia społecznego, będąc przy tym także towarem o wymiernej wartości (Golka, 2005, s. 253–265). Warto przy tym zauważyć, że społeczeństwo informacyjne zależy nie tylko od samej informacji, ale także od środków jej gromadzenia i przesyłania – czyli komunikacji, której zasadniczym elementem stała się cała nowo powstała sfera cyberprzestrzeni.

Chociaż informacja była ważna dla człowieka od wczesnych etapów rozwoju społeczeństw, to dopiero połączenie rewolucji technologicznej przełomu XX oraz XXI w., w tym przede wszystkim upowszechnienie dostępu do sieci Internet w skali globalnej, z rozwojem gospodarki rynkowej z jednej strony nadało informacji dodatkową, unikalną wartość, zaś z drugiej, umożliwiło przełom społeczny i wyodrębnienie się społeczeństwa informacyjnego. Stosunkowo szybko zauważono przy tym, że wszelkiego rodzaju pozytywnym skutkom rozwoju nowej formy społeczeństwa towarzyszą zagrożenia – zarówno zupełnie nowe, dotąd niespotykane i swoiste dla sfery cyberprzestrzeni, jak i takie, które stanowią przeniesione do tej sfery formy dobrze znanych czynów społecznie nagannych i niepożądanych (Goban-Klas i in., 1999, s. 42–43, 64–72).

Cyberprzestrzeń, będąca pojęciem stworzonym w 1984 r. i upowszechnionym przez pisarza science-fiction Williama Gibsona, niezależnie od wielu konkurujących ze sobą definicji wypracowanych na arenie międzynarodowej, została zdefiniowana w Polsce ustawowo. Jest to zatem przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania), wraz z powiązaniami między nimi oraz relacjami z użytkownikami (Wasilewski, 2013, s. 225–234). Wraz z dynamicznym rozwojem cyberprzestrzeń stała się – co należy uznać ze społecznego punktu widzenia za

proces o charakterze naturalnym – źródłem nowych zagrożeń oraz środowiskiem, do którego nastąpiła szeroko zakrojona migracja wszelkich aktywności o charakterze przestępczym. Jest to więc nowa, w dużej części nadal nierozpoznana sfera stanowiąca prawdziwe wyzwanie dla organów ścigania oraz wszelkich instytucji odpowiedzialnych za zapewnianie bezpieczeństwa i porządku publicznego. Zgodnie z doktryną współczesnej kryminalistyki, uznającej prewencję i zapobieganie przestępczości za podstawową funkcję tej nauki (Gruza i in., 2008, s. 23–24), niezwykle ważne staje się w tym kontekście wypracowanie skutecznych, skierowanych do szerokich grup społecznych programów zapobiegania zagrożeniom w cyberprzestrzeni opartych na informacji oraz edukacji. Takie działania, nakierowane bezpośrednio na użytkowników sieci, powinny stanowić uzupełnienie i wzmocnienie szeroko wdrażanych narzędzi oraz rozwiązań technologicznych o charakterze zarówno programowym, jak i sprzętowym, służących zapewnianiu bezpieczeństwa cyberprzestrzeni.

Analiza aspektów bezpieczeństwa cyberprzestrzeni

Problematyka bezpieczeństwa cyberprzestrzeni jest niewątpliwie zagadnieniem bardzo kompleksowym, wielowątkowym, które można analizować w różnych aspektach. Można je postrzegać w ujęciu *stricte* technologicznym, koncentrując się na rozwoju narzędzi programowych oraz coraz bardziej zaawansowanych rozwiązań sprzętowych związanych z infrastrukturą oraz urządzeniami dostępowymi, których funkcją jest zapewnienie transmisji danych w sieci Internet. W praktyce sfera ta jest domeną globalnych producentów urządzeń telekomunikacyjnych, zaś osiągane w niej postępy związane są aktualnie ściśle z pracami międzynarodowych organizacji standaryzacyjnych, takich jak Europejski Instytut Standaryzacji w Telekomunikacji (ETSI) czy Międzynarodowy Związek Telekomunikacyjny (ITU), wypracowujących uznawane przez sektor telekomunikacyjny standardy techniczne, wdrażane w skali globalnej zarówno przez producentów sprzętu, jak i operatorów telekomunikacyjnych oferujących stacjonarne i mobilne usługi dostępu do sieci Internet.

Kolejnym popularnym ujęciem analitycznym przedmiotowej problematyki jest rozpatrywanie jej z punktu widzenia regulacji prawnych – zarówno

krajowych, jak i międzynarodowych. Zagadnieniem o zasadniczym znaczeniu w tym kontekście jest określenie normatywnych definicji czynów wywołujących zagrożenia cyberprzestrzeni. Aktem prawa międzynarodowego, który w sposób szczególny wpłynął na kształtowanie narodowych regulacji karnych dotyczących cyberprzestępstw w krajach Unii Europejskiej, jest niewątpliwie Konwencja Rady Europy o cyberprzestępczości z 2001 r. (tzw. konwencja budapesztańska), ratyfikowana również przez Polskę w roku 2014. Konwencja ta przede wszystkim definiuje normatywnie podstawowe pojęcia związane z cyberprzestrzenią, takie jak „system informatyczny" czy „dane informatyczne". Zawiera również katalog czynów popełnianych w cyberprzestrzeni, które państwa członkowskie są zobowiązane uznać za przestępstwa. Katalog ten podzielony jest na cztery kategorie:

- przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów,
- przestępstwa komputerowe,
- przestępstwa ze względu na charakter zawartych informacji (tzw. kontentowe),
- przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

W podobny sposób czyny wymierzone w bezpieczeństwo cyberprzestrzeni określone są w Dyrektywie Parlamentu Europejskiego i Rady 2013/40/UE z 2013 r. dotyczącej ataków na systemy informatyczne, która stanowiąc obowiązujący akt prawotwórczy, jest szczególnie istotna z krajowego punktu widzenia (Aleksandrowicz, 2016, s. 11–25).

Konsekwentnym następstwem m.in. przywołanych powyżej regulacji o charakterze międzynarodowym jest unormowanie niepożądanych zachowań w cyberprzestrzeni na gruncie krajowym. Najbardziej niebezpieczne z nich zostały stypizowane w ustawie Kodeks karny, co *de facto* wyznaczyło granice swobodnego poruszania się w cyberprzestrzeni. Należy przy tym zauważyć, że przepisy karne znajdujące zastosowanie do przypadków łamania prawa w tej sferze zawarte są również w wielu ustawach szczególnych, w tym w ustawie o prawie autorskim i prawach pokrewnych określającej zasady odpowiedzialności karnej z tytułu naruszania praw autorskich (Lis, 2014,

s. 241–256). Chociaż analiza poszczególnych cyberprzestępstw wykracza dalece poza ramy niniejszej publikacji, to istotne wydaje się przedstawienie za J. Kosińskim zestawu cech wspólnych, trafnie i uniwersalnie ujmujących cyberprzestępczość jako zachowania o następującej specyfice:

- przedmiotem, środkiem lub celem zamachu są komputer, sieć komputerowa, urządzenie teleinformatyczne,
- przestępcy wykorzystują do swoich działań łatwą w obsłudze a jednocześnie zaawansowaną technologię,
- zapewniona jest anonimowość sprawcy,
- przestępca komputerowy jest traktowany przez społeczeństwo jako człowiek nieszkodliwy,
- ofiara jest często nieświadoma, że jej system został zaatakowany,
- rzadko składane są doniesienia o popełnieniu cyberprzestępstw, chyba że doszło do znacznych strat finansowych,
- do popełnienia przestępstwa wystarczy krótki czas,
- przestępstwa pociągają niskie koszty, a przynoszą duże korzyści,
- zorganizowanie i specjalizacja zachowań przestępczych – często jest to działanie na zlecenie,
- międzynarodowy zasięg, transgraniczność,
- asymetryczność zagrożeń,
- w większości są to czyny, które nie są nakierowane na indywidualną ofiarę, a raczej na wybraną grupę, np. klientów banku (Kosiński, 2015, s. 45–46).

Bezpieczeństwo cyberprzestrzeni jest także kwestią często podejmowaną i analizowaną z punktu widzenia całego państwa, jako nabierający znaczenia element szerszego pojęcia bezpieczeństwa narodowego, i w powiązaniu z wynikającymi z przeobrażeń technologicznych potrzebami ochrony elementów infrastruktury publicznej dostępnych bezpośrednio lub pośrednio poprzez sieci teleinformatyczne – tzw. infrastruktury krytycznej. Zaliczane są do niej takie elementy infrastruktury, które decydują o ciągłości funkcjonowania państwa i społeczeństwa – w tym te zapewniające zaopatrzenie w wodę, energię, łączność czy zasoby informacyjne. Potrzeba zapewnienia bezpieczeństwa cybernetycznego państwa jest związana z postrzeganiem cyberprzestrzeni

jako nowego środowiska walki, w którym będą się toczyły (a w pewnym zakresie już się toczą) konflikty militarne i pozamilitarne przyszłości, wymagające opracowania przez państwo zupełnie nowych strategii oraz narzędzi służących toczeniu cyberwojen, zastępujących tradycyjne pole walki. Dodatkowo istotnym elementem konfliktów w cyberprzestrzeni staje się, jak pokazuje już doświadczenie ostatniej dekady, walka informacyjna. Jest to zjawisko występujące samoistnie, w warunkach formalnego pokoju, w którym cele nie mają bezpośredniego znaczenia militarnego, zaś działania (ataki) prowadzone w środowisku cyberprzestrzeni mogą wywoływać zagrożenia dla bezpieczeństwa międzynarodowego w skali globalnej, destabilizację infrastruktury krytycznej, zakłócenia w funkcjonowaniu administracji, straty gospodarcze spowodowane zahamowaniem rozwoju gospodarki i przedsiębiorstw, a także wymierne straty osobiste obywateli (Aleksandrowicz, 2014, s. 39–52).

Odrębnym wzmagającym się zagrożeniem dla państwa i obywateli, specyficznym dla cyberprzestrzeni i wymagającym odnotowania, jest cyberterroryzm. Mając na uwadze wspomniany już wcześniej fakt, że aktualnie istotna część infrastruktury i systemów związanych z codziennym funkcjonowaniem naszej cywilizacji jest osiągalna poprzez sieć, należy stwierdzić, iż stanowi ona atrakcyjny potencjalny obiekt ataku terrorystycznego, który może pociągnąć za sobą realne ofiary w ludziach (Marczak, 2014, s. 147–163). Ponadto narzędzia komunikacyjne dostępne w sieci Internet – w tym przede wszystkim media społecznościowe o globalnym zasięgu – stanowią efektywne narzędzia zarówno dla propagowania ideologii terrorystycznej oraz koordynacji działań podejmowanych przez rozproszone komórki terrorystyczne, jak i prowadzenia w cyberprzestrzeni wojny informacyjnej dla realizacji celów organizacji terrorystycznych.

Problematyka bezpieczeństwa cyberprzestrzeni powinna być wreszcie analizowana z punku widzenia jej użytkowników, stanowiących, jak się okazuje, newralgiczną grupę, będącą w istocie z jednej strony źródłem większości zagrożeń, zaś z drugiej stanowiącą gros ofiar wszelkich niepożądanych zjawisk w świecie wirtualnym. Podstawowymi problemami, jakie należy wskazać w tym kontekście, jest brak świadomości zagrożeń oraz podejmowanie działań zarówno lekkomyślnych, jak i łamiących wszelkie zalecenia oraz standardy bezpieczeństwa. Żadne, nawet najbardziej wyrafinowane techno-

logie oraz procedury bezpieczeństwa nie spełnią swojej roli, jeżeli zawiedzie ich użytkownik – człowiek stanowiący przysłowiowe najsłabsze ogniwo w całym systemie (Lech i in., 2008, s. 241–242). Dodatkowymi kwestiami potęgującymi istniejące zagrożenia są specyfika cyberprzestrzeni, wymagająca pewnego minimum wiedzy technicznej dla ich rozpoznania i unikania, a także wspomniana już wcześniej specyficzna natura niektórych cyberprzestępstw wykorzystujących urządzenia dostępowe do sieci bez jakiejkolwiek świadomości ich użytkownika. Stąd narastająca i pilna potrzeba dostarczenia szerokiej rzeszy użytkowników odpowiedniego zasobu informacji (wiedzy) pozwalającej na bezpieczne poruszanie się w cyberprzestrzeni, która może być zrealizowana w ramach stosownych, właściwie sprofilowanych programów o charakterze edukacyjnym (Domański, 2013, s. 69–85).

Strategie bezpieczeństwa cyberprzestrzeni UE oraz RP

Wyrazem uznania problematyki zagrożeń cyberbezpieczeństwa i skutecznego przeciwdziałania temu zjawisku jest opracowywanie na przestrzeni ostatniej dekady strategii cyberbezpieczeństwa zarówno na forum organizacji międzynarodowych o charakterze globalnym i regionalnym, jak i w poszczególnych państwach. Pośród wielu opublikowanych dokumentów o takim charakterze najistotniejsze znaczenie z krajowego punktu widzenia mają te opracowane na forum Unii Europejskiej, jak również w samej Polsce.

Podstawą aktualnych działań UE w zakresie bezpieczeństwa cyberprzestrzeni jest komunikat Komisji Europejskiej z dnia 7 lutego 2013 r. pt. *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*. Określono w jej ramach zarówno strategiczne cele, jak i konkretne działania nakierowane na uzyskanie odporności cybernetycznej, ograniczenie cyberprzestępczości i ustanowienie wspólnej polityki dotyczącej cyberprzestrzeni. Kolejnymi istotnymi krokami podjętymi przez UE było przyjęcie Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. Dyrektywa NIS – UE 2016/1148), komunikatu Komisji Europejskiej pt. *Wzmacnianie europejskiego systemu odporności cybernetycz-*

nej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego, a także ostatnio tzw. pakietu cyberbezpieczeństwa [COM(2017) 477]. Wśród celów tego ostatniego dokumentu podkreśla się potrzebę podnoszenia poziomu świadomości obywateli i przedsiębiorstw w zakresie bezpieczeństwa cybernetycznego, a także istotne wzmocnienie mandatu powołanej jeszcze w 2004 r. Europejskiej Agencji ds. Bezpieczeństwa Cyberprzestrzeni (ENISA), która ma się stać m.in. centrum eksperckim zbierającym i udostępniającym informacje o zagrożeniach w cyberprzestrzeni obywatelom krajów członkowskich Unii.

Na gruncie krajowym począwszy od przyjętej przez rząd w 2013 r. Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, będącej pierwszym dokumentem o charakterze strategicznym dotyczącym cyberbezpieczeństwa, przedstawiane są kolejne strategie cyberbezpieczeństwa Rzeczypospolitej Polskiej. Aktualna edycja to dokument na lata 2017–2022 przedstawiony w bieżącym roku przez Ministerstwo Cyfryzacji. W zakresie przedmiotu zainteresowania niniejszej publikacji *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022* formułuje cel szczegółowy – stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli. Ma być on osiągnięty za pomocą edukacji w zakresie cyberbezpieczeństwa już na etapie kształcenia wczesnoszkolnego, w tym wdrożenia stosownych zmian w podstawach programowych nauczania, kampanii społecznych i działań uwrażliwiających społeczeństwo na zagrożenia płynące z w cyberprzestrzeni, a także działań edukacyjnych w zakresie praw i wolności w środowisku cyfrowym. Administracja publiczna ma wspierać wszelkie działania, zarówno operatorów usług kluczowych, jak i dostawców usług cyfrowych, w zakresie podejmowania przedsięwzięć edukacyjnych i informacyjnych dla zapewnienia użytkownikom końcowym dostępu do wiedzy pozwalającej na zrozumienie zagrożeń w cyberprzestrzeni i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami (*Strategia*…, 2017, s. 23).

Koncepcja projektu w zakresie informowania i edukacji użytkowników cyberprzestrzeni

Według najnowszego badania Gemius/PBI (pbi.org.pl) liczba internautów w Polsce w listopadzie 2017 r. wyniosła ogółem 27,7 mln, z czego z kom-

puterów osobistych i laptopów korzysta 24,2 mln osób, a z urządzeń mobilnych – 21,5 mln. Ta ogromna rzesza użytkowników narażona jest permanentnie na różnego rodzaju zagrożenia w cyberprzestrzeni, przedstawione w ramach niniejszego opracowania, co dostrzegane jest zarówno w formułowanych na arenie krajowej i międzynarodowej dokumentach o charakterze strategicznym, jak i przez samych zainteresowanych. Oceniając problem braku należytej informacji i edukacji, które mogłyby być skutecznymi narzędziami zapobiegania cyberzagrożeniom, z punktu widzenia użytkowników sieci warto wskazać na dane przedstawione w dorocznym wystąpieniu Przewodniczącego Komisji Europejskiej w dniu 13 września 2017 r. – wg 86% użytkowników Internetu w krajach członkowskich UE rośnie zagrożenie stania się ofiarą cyberataku, podczas gdy 51% tej populacji nie czuje się w ogóle lub czuje się nieadekwatnie poinformowane o cyberzagrożeniach (Juncker, State of Union Address, 2017). W sposób oczywisty uzasadnia to podejmowanie inicjatyw o charakterze informacyjnym oraz edukacyjnym w przedmiotowym zakresie.

Warto zatem zainicjować kompleksowe przedsięwzięcie służące opracowaniu systemu edukacji dotyczącego cyberprzestrzeni – dla stworzenia powszechnej kultury funkcjonowania w cyberprzestrzeni, a także dostarczania informacji i promowania pozytywnych wzorców funkcjonowania w tym środowisku. Powyższe miałoby na celu:

- dążenie do poszerzania świadomości społecznej w zakresie właściwego postrzegania cyberprzestrzeni oraz zwiększenia kompetencji użytkowników i umiejętności korzystania z Internetu w obecnym świecie,
- edukowanie szerokich grup społecznych w obszarze zagrożeń występujących w wirtualnym świecie,
- dotarcie z wiedzą i informacją do jak największego grona odbiorców, w szczególności do grup objętych wykluczeniem cyfrowym (np. ze względów geograficznych, społecznych itp.).

Projekt taki powinien być całkowicie neutralny technologicznie, co wyzwoli go z wielu ograniczeń i problemów związanych z przypisaniem do określonych rozwiązań technicznych powiązanych z konkretnymi producentami infrastruktury sieciowej. Istotą są zatem treści projektu, a nie wykorzystywane medium transmisyjne czy urządzenie dostępowe. Rezultaty projektu

powinny przejawiać się w formie programów nauczania oraz innych materiałów edukacyjnych dla szkół na różnych poziomach nauczania, kursów edukacyjnych online, stworzenia portalu edukacyjnego powiązanego z platformą szkoleniową, a także opracowaniem stosownych aplikacji na urządzenia mobilne. Uczestnikami proponowanego projektu, ze względu na potrzebę dotarcia z treściami informacyjnymi oraz edukacyjnymi do jak najszerszych grup użytkowników cyberprzestrzeni, powinny być zarówno kompetentne instytucje edukacyjne (szkoły wyższe), instytucje badawczo-rozwojowe, właściwe instytucje publiczne związane z problematyką edukacji oraz cyberprzestrzeni, jak i sektor prywatny – posiadające szeroką bazę klientów firmy dostarczające usługi dostępu do sieci Internet.

Wnioski

Informacja i edukacja są niewątpliwie środkami przeciwdziałania zagrożeniom w cyberprzestrzeni, środkami, na które istnieje duże, potwierdzone badaniami zapotrzebowanie ze strony użytkowników sieci Internet. Deficyt w tym zakresie, mimo dostrzegania potrzeby propagowania informacji dotyczących cyberprzestrzeni w strategicznych dokumentach rządowych i sporządzanych przez organizacje międzynarodowe, potwierdza potencjał, jaki mogą nieść przemyślane i kompleksowe propozycje programów edukacyjnych postrzeganych jako element prewencji i zapobiegania zagrożeniom cyberprzestrzeni.

Dokonując syntezy powyższych rozważań, należy stwierdzić, iż zasadne jest przedstawienie koncepcji wykorzystania systemu edukacji pozaformalnej, opartej o wdrażany aktualnie w naszym kraju mechanizm sektorowych rad ds. kompetencji, jako optymalnego rozwiązania służącego dostarczeniu w wymiarze powszechnym informacji oraz edukacji użytkownikom cyberprzestrzeni w Polsce. Mechanizm ten posiada wyjątkowe zalety, wynikające z faktu oparcia go o zasadę ścisłej współpracy dwóch grup podmiotów istotnych dla informowania oraz edukowania o zagrożeniach występujących w cyberprzestrzeni – podmiotów akademickich oraz gospodarczych (zarówno podmiotów komercyjnych, jak i organizacji samorządu gospodarczego i organizacji pozarządowych). Istotą funkcjonowania sektorowych rad ds. kompetencji jest tworzenie formalnie zatwierdzanych i następnie certyfikowanych przez państwo

ram kwalifikacyjnych oraz poszczególnych kwalifikacji (kompetencji), które można odnieść do ustalonych poziomów nauczania w ramach powszechnego systemu edukacji formalnej – szkolnictwa powszechnego oraz wyższego. Jego podstawową zaletą jest fakt możliwości łączenia edukacji o charakterze wysokospecjalistycznym w zakresie bezpieczeństwa cyberprzestrzeni z edukacją o charakterze powszechnym na poziomie podstawowym, niezbędnej szerokim rzeszom użytkowników cyberprzestrzeni. Mechanizm taki stanowi dla podmiotów komercyjnych idealną okazję dla realizacji społecznej odpowiedzialności biznesu, a także pozwala na uzyskanie realnego wpływu na programy nauczania i kompetencje nabywane dzięki prowadzonym działaniom edukacyjnym w ramach edukacji pozaformalnej. Podmioty i środowiska akademickie mogą zarówno dostosować przekazywane kompetencje do aktualnych potrzeb i wymagań rynku, jak i wdrożyć szeroko zakrojone działania szkoleniowe adresowane do grup podwyższonego ryzyka, którymi w przypadku cyberprzestrzeni będą np. dzieci oraz młodzież szkolna czy seniorzy, a także stosownie certyfikować nabyte kompetencje.

Praktyczna realizacja przedstawionej koncepcji wymaga powołania stosownej sektorowej rady ds. kompetencji w ramach sektora technologii informacyjnych oraz komunikacyjnych (ICT) z udziałem wiodących przedstawicieli sektora komercyjnego oraz samorządu gospodarczego, uczelni wyższych oraz instytutów naukowo-badawczych zainteresowanych edukacją w zakresie różnych aspektów bezpieczeństwa cyberprzestrzeni – o charakterze zarówno specjalistycznym, jak i powszechnym. Należy się przy tym spodziewać akceptacji przedstawionej koncepcji przez instytucje i organy państwa zainteresowane problematyką cyberbezpieczeństwa. Jak się wydaje, w chwili obecnej zaistniały już zatem warunki umożliwiające zainicjowanie takiego przedsięwzięcia.

Warto też zauważyć, że wartością dodaną związaną z realizacją zaproponowanej koncepcji może być stworzenie podstawy do budowania kultury funkcjonowania użytkownika (a także całego społeczeństwa) w cyberprzestrzeni, a więc projektu zakrojonego znacznie szerzej niż tylko jako przeciwdziałanie poszczególnym zagrożeniom w rzeczywistości wirtualnej, pozwalającego przede wszystkim młodemu pokoleniu na harmonijne łączenie od najmłodszych lat dwóch jakże odmiennych światów, w których przychodzi mu *de facto* codziennie funkcjonować.

Literatura

Aleksandrowicz, T.R. (2016). *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 15(8), s. 11–25, ISSN: 2080-135.

Aleksandrowicz, T.R. (2014). *Strategie bezpieczeństwa w cyberprzestrzeni. Cyberwojny*. W: K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa: Wydawnictwo Difin, s. 39–52, ISBN: 9788379302727.

Chmura, J. (2016). *Wartość informacji i jej bezpieczeństwo w gospodarce opartej na wiedzy,* „Journal of Modern Science" 3/30. ISSN 1734-2031.

Domański, Z. (2013). *Zagrożenia w cyberprzestrzeni.* W: M. Such-Pyrgiel (red.), *Bezpieczeństwo społeczne w XXI wieku w ujęciu socjologicznym, pedagogicznym, prawnym i nauk o zarządzaniu*. Józefów: Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi. ISBN 9788362753376.

European Commission, *Cybersecurity. State of the Union 2017*, 2017, s. 1–2.

Goban-Klas, T., Sienkiewicz, P. (1999). *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków: Wydawnictwo Postępu Rozwoju Telekomunikacji, s. 42–43, 64–72, ISBN: 8386476192.

Golka, M. (2005). *Czym jest społeczeństwo informacyjne*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny", rok 67, z. 4, s. 253–265, ISSN: 0035-9170.

Gruza, E., Goc, M., Moszczyński, J. (2008). *Kryminalistyka – czyli rzecz o metodach śledczych*, Warszawa: Wydawnictwa Akademickie i Profesjonalne, s. 23–24, ISBN: 9788360807101.

Kosiński, J. (2015). *Paradygmaty cyberprzestępczości*, Warszawa: Wydawnictwo Difin, s. 45–46, ISBN: 9788379306664.

Lech, T., Podgórski, G. (2008). *Bezpieczeństwo w sieci*. W: J. Papińska-Kacperek (red.), *Społeczeństwo informacyjne*, Warszawa: Wydawnictwo Naukowe PWN, s. 241–242, ISBN 9788301154073.

Lis, W. (2014). *Bezpieczeństwo w cyberprzestrzeni w ujęciu prawnokarnym – wybrane zagadnienia*, „Rocznik Bibliologiczno-Prasoznawczy", t. 6/17, Kielce, s. 241–256, ISSN: 1231-0972

Marczak, P. (2014). *Cyberataki – narzędzia konfliktu w cyberprzestrzeni*. W: K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa: Wydawnictwo Diffin, s. 147–163, ISBN: 9788379302727.

Sitek, M. (2017). *The human rights to communicate in the light of the development of IT technology at the turn of the XX and XXI centurie*. W: M. Sitek, A.F. Uricchio, I. Florek (red.), *Human rights between needs and possibilities*, Józefów: Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide de Gasperi, s. 257–270. ISBN 9788362753857.

Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, Ministerstwo Cyfryzacji, Warszawa 2017, s. 23.

Wasilewski, J. (2013). *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 9(5), s. 225–234, ISSN: 2080-135.